UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re	:	Chapter 11
CELSIUS NETWORK LLC, *et al.*	:	Case No. 22-10964 (MG)
	:	(Jointly Administered)
Debtors.[1]	:	

CONSUMER PRIVACY OMBUDSMAN

FIRST REPORT TO THE COURT

January 27, 2023

Lucy L. Thomson
Consumer Privacy Ombudsman

The Willard; Suite 400
1455 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
Telephone: (703) 212-8770

[1] The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 121 River Street, PH05, Hoboken, New Jersey 07030.

TABLE OF CONTENTS

I. Privacy Ombudsman Report to the Court

A. Overview of the Privacy Issues

Pursuant to Bankruptcy Code section 332(b), Lucy L. Thomson, the Consumer Privacy Ombudsman ("CPO" or "Ombudsman") appointed in this case,[2] submits this Report to advise the Court on the issues related to the protection of the privacy of consumers ("account holders") of Celsius Network LLC ("Debtors" or "Celsius").

The Bankruptcy Code provides a framework in sections 332 and 363 for evaluating the sale or transfer of personal consumer records in the context of a bankruptcy case. 11 U.S.C. §§ 101 *et. seq*. The statute provides a broad mandate for the Ombudsman – to investigate and provide the Court with information relating to:

- The Debtors' Privacy Policy;
- Potential losses or gains of privacy to consumers if the sale is approved;
- Potential costs or benefits to consumers if the sale is approved; and
- Possible alternatives that would mitigate potential privacy losses or costs to consumers.

11 U.S.C. § 332.

In enacting sections 332 and 363, Congress has evidenced its intention to protect the privacy interests of consumers in connection with the bankruptcy sale of personal data. When the Court ordered the appointment of the Ombudsman, he stated the need to ensure that any sale

[2] United States Trustee, Notice of Appointment of Consumer Privacy Ombudsman, October 25, 2022 [ECF No. 1190, filed 10/25/22]; Order Approving the Appointment of a Consumer Privacy Ombudsman, October 27, 2022 [ECF No. 1208, filed 12/27/22]. "[T]he Court has discretion to appoint an ombudsman if it believes a neutral third party would be helpful, even if a sale will comply with the Debtors' privacy policy. Here, given the significant amount of potential customer data that could be included in a sale, the Court finds that appointing a neutral Consumer Privacy Ombudsman early in the sale process will ensure that any sale adequately protects such customer data. 3 COLLIER ON BANKRUPTCY ¶ 332.02 (16th ed. 2022)." page 24 [ECF No. 1167, filed 10/24/22]. The Ombudsman has served as the CPO in 33 prior bankruptcy cases where privacy issues related to the sale of personal data were addressed.

"adequately protects the significant amount of potential customer data that could be included in the sale" of the retail platform assets. The Bankruptcy Code provides that in making that determination, the Court may: (1) consider whether the sale is consistent with the privacy policy; (2) give due consideration to the facts, circumstances, and conditions of such sale; and (3) find that no showing was made that such sale would violate applicable non-bankruptcy laws.[3] 11 U.S.C. § 363(b)(1).

The Ombudsman worked with counsel for the Debtors and members of the Celsius staff. They cooperated fully, participating in calls and providing the information needed for this CPO Report. Clearly, the collaborative process we have been engaged in has been productive. In this case, for the benefit of all stakeholders, the Debtors have actively pursued a dual-track process of marketing all of their assets for sale while simultaneously developing a path towards a standalone reorganization.

While the sale or transfer of digital assets to a new entity may present some novel issues for the Court, established principles of privacy protection[4] provide a roadmap for the Court when

[3] The CPO Process – Section 363(b)(1) of the Bankruptcy Code provides that the Court must make a number of determinations before the Debtors are authorized to sell the Celsius personally identifiable consumer records. More specifically:

- If the Debtors' Privacy Policy prohibits the transfer of personally identifiable information about individuals to persons that are not affiliated with the Debtors; and
- If the policy is in effect on the date of the commencement of the case;
- Then the Trustee may not sell personally identifiable information to any person unless–

  (A) such sale is consistent with such policy; or

  (B) after appointment of a consumer privacy ombudsman in accordance with section 332, and after notice and a hearing, the court approves such sale or such lease –

  (i) giving due consideration to the facts, circumstances, and conditions of such sale; and

  (ii) finding that no showing was made that such sale would violate applicable non-bankruptcy law.

[4] The Fair Information Practice Principles (FIPPs) are fundamental to privacy laws today. The widely-accepted FIPPs serve as the backbone of the federal Privacy Act of 1974, are core to FTC regulatory actions, and are mirrored in the laws of many U.S. states, countries, and international organizations.

addressing the privacy issues in this case. Personal data should not only be protected from undue risks of data breaches that could subject consumers to identity theft and fraud, its collection, use, and sale or transfer should be limited to the "minimum necessary" to achieve the Purchaser's business objectives and deleted as soon as it is no longer needed in accordance with an appropriate data retention schedule. Finally, practical approaches for protecting privacy in prior bankruptcy cases can provide appropriate solutions the Court and the parties may wish to adopt.

The major banking laws do not comprehensively regulate the collection, use, and sale of consumers' personal and financial data.[5] As a result, these statutes and regulations provide little guidance on the measures necessary to protect the privacy of the Celsius account holders. On the other hand, the Dodd-Frank Act (2010)[6] prohibits unfair, deceptive, or abusive acts or practices for consumer financial products and services. Section 5 of the Federal Trade Commission Act (FTC Act) similarly prohibits unfair and deceptive acts or practices and has been the basis for FTC decisions finding privacy violations in many cases and providing privacy-related recommendations in bankruptcy cases over many years.

Comprehensive privacy protections are provided in some U.S. state privacy and data protection laws, as well as the European Union (EU) General Data Protection Regulation (GDPR) and country privacy laws. The Celsius privacy policy sets forth more far-reaching privacy protections for residents of California, as well as the 27 EU countries, than for the other

[5] Recognizing the inadequacy of the federal privacy protections, President Joseph Biden called on members of Congress to "pass legislation to hold big technology and social-media companies accountable, accusing some in the industry of exploiting users' personal data and endangering children."

Biden Calls for Limiting Tech Companies' Use of Personal Data, Targeted Ads: Both parties have criticized social-media companies, WALL STREET JOURNAL (Jan. 11, 2023), https://www.wsj.com/articles/biden-calls-for-limiting-tech-companies-use-of-personal-data-targeted-ads-11673469013

[6] Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010 (Dodd-Frank Act), P.L. 111-203.

account holders. As a result, it affords different privacy protections to account holders based on where they live. (The Celsius privacy policy is included in this Report as Appendix A).

In the context of bankruptcy cases, Courts have recognized that a balance must be reached between the sale of an entire company, along with vast amounts of personal records, and protection of the privacy rights of consumers – the account holders. Factors that have been considered in establishing that balance include the status of the customer accounts (active or inactive), geographic location of the account holders, nature and sensitivity of the personal data collected and maintained by Celsius, expectations of privacy, and practical steps the parties can take to protect the privacy of account holders and their personal and financial data.

The January 3, 2023 *Joint Statement on Crypto-Asset Risks to Banking Organizations* published by the three leading federal banking agencies provides context for the recommendations provided in this CPO Report.[7] The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) observed that the "events of the past year have been marked by significant volatility and the exposure of vulnerabilities in the crypto-asset sector." The statement highlights eight crypto-asset[8] risks, many of which affected and may have harmed retail investors and consumers.[9] (The Joint Statement is included in this Report as Appendix B).

---

[7] Federal Reserve Board, https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230103a1.pdf. ["Banking Regulators Joint Statement."]

[8] By "crypto-asset," the agencies refer generally to any digital asset implemented using cryptographic techniques.

[9] The following are four of the risks highlighted in the Banking Regulators Joint Statement:

- Legal uncertainties related to custody practices, redemptions, and ownership rights, some of which are currently the subject of legal processes and proceedings.
- Inaccurate or misleading representations and disclosures by crypto-asset companies, including misrepresentations regarding federal deposit insurance, and other practices that may be unfair, deceptive, or abusive, contributing to significant harm to retail and institutional investors, customers, and counterparties.
- Risk management and governance practices in the crypto-asset sector exhibiting a lack of maturity and robustness.

This First Consumer Privacy Ombudsman (CPO) Report to the Court ("CPO Report") presents the "facts, circumstances, and conditions" of a potential sale or transfer of the personal and financial data of the 1.7 million Celsius account holders by analyzing the potential gains or losses of privacy and the costs or benefits to consumers if the sale is approved. It highlights key issues for the Court's consideration and discusses them in detail in the sections that follow.

In lieu of an outright sale to a third party and/or a potential competitor, the Debtors are developing a plan for the creation of a new public corporation with professional management. Through a "recovery corporation," the value of the Debtors' assets, including the Debtors' liquid and illiquid cryptocurrency, loan receivables, mining assets, and proceeds from litigation claims, would be distributed to account holders. [ECF No. 1940, filed 1/26/23]

Taking into consideration this new proposal, Section V presents alternatives that could mitigate potential privacy losses or costs to consumers. Section VI identifies and analyzes the relevant non-bankruptcy laws. Further, the CPO Report recommends steps the parties should take to appropriately retain and dispose of personal data not included in the sale or transfer to a new entity, and to comply with the U.S. states and global privacy and data protection laws.

The Ombudsman will work with the parties to help develop specific plans for the privacy protection of account holders' data once decisions concerning the Debtors' proposed sale or transfer of the retail platform assets have been finalized.

- Heightened risks associated with open, public, and/or decentralized networks, or similar systems, including, but not limited to, the lack of governance mechanisms establishing oversight of the system; the absence of contracts or standards to clearly establish roles, responsibilities, and liabilities; and vulnerabilities related to cyber-attacks, outages, lost or trapped assets, and illicit finance.

Banking Regulators Joint Statement*, supra* note 7.

1. Personal Data About Account Holders Collected and Maintained by Celsius

In the conduct of its business, Celsius collected and maintained an enormous amount of sensitive personal and financial data about all 1.7 million current account holders and individuals with inactive accounts.[10] The vast amount of data collected by Celsius makes privacy a particularly important factor in considering approval of any sale or transfer because the personal data is highly sensitive.

Because, according to the Celsius privacy policy, the personal data was used for marketing company products and serving ads to account holders in addition to conducting financial transactions related to cryptocurrency, the data encompasses confidential information about many aspects of consumers' daily lives and their activities, including their social media contacts and biometric and geolocation data. As well, it includes confidential account numbers and financial records that must be protected.

The Celsius privacy policy states that "[w]hen we use the term "Personal Information" we mean any information about an individual from which that person can be identified."[11] The privacy policy further defines "personal information" broadly in the section on Sources of Personal Information**:** "For the avoidance of doubt, if we combine Personal Information with non-personal information, the combined information will be treated as Personal Information as long as it remains combined."

[10] The company reported that as of July 2022 Celsius had approximately 1.7 million registered users and 300,000 active users with account balances of more than $100. Declaration of Alex Mashinsky, Chief Executive Officer of Celsius Network LLC, In Support of Chapter 11 Petitions and First Day Motions, ¶ 9 [ECF No. 23, filed 7/14/22] ["Mashinsky Declaration I"].

[11] Section 101 (41A) of the Bankruptcy Code defines the term "personally identifiable information" more narrowly than the Celsius privacy policy, *e.g.*, to include name, address, e-mail, telephone number, Social Security number, credit card number, and if in addition to those items, birth date, birth certificate number, or place of birth; or "any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically."

2. Different Privacy Solutions for Categories of Account Holders May Be Required

Analysis of the account status and geographic location of Celsius users is required to arrive at appropriate privacy solutions. Depending on the type of transaction the Debtors propose, it may be reasonable to include individuals with active accounts in the sale or transfer and exclude those whose accounts are inactive.

As the data presented in the following table illustrates, of the 1.7 million total account holders, more than 600,000 have active accounts and approximately 1.1 million accounts are inactive. Celsius account holders reside in all 50 states and U.S. territories. More than 370,000 active users reside in 200+ countries around the globe, including all 27 EU countries. Many are covered by a variety of U.S. state and EU and country data privacy laws that govern how their data is processed and protected by Celsius.

Celsius Account Holders			
Total = 1.7 million			
Active Users		**Inactive Accounts**	
603,328 all active accounts		~ 1.1 million	
300,000+ with account balances > $100			
U.S. – 50 States and Territories	**Global** 200 Countries	**U.S.**	**Global**
232,162 users	371,166 users	~ 600,000 users	~ 500,000 users
Top Five: California, Florida, Texas, N.J., Illinois	*Top Five*: Australia, Canada, U.K., France, Italy		
	150,000+ users located in the 27 EU countries		
Non-bankruptcy Laws that Apply			
U.S., 50 State privacy and data protection	GDPR and Country laws	U.S., 50 State privacy and data protection	GDPR and Country laws
Comprehensive U.S. State privacy laws: CA, VA, 7/23: CO, CT 64,817 users		Comprehensive U.S. State privacy laws: CA, VA, 7/23: CO, CT	

3. "Qualified Buyer" Criteria and Practical Steps to Protect Privacy in Prior Cases

Initially, bankruptcy courts have assessed whether the proposed Purchaser is a "Qualified Buyer," using criteria created in 2008 and first applied in the *Toysmart* case.[12] These criteria have been updated and followed in many subsequent bankruptcy cases for more than a decade.[13]

Practical steps the parties have taken in prior bankruptcy cases to protect the privacy of personal data involve creating a targeted sale that included only the consumers' records required for the particular business purposes and requirements of the Purchaser, and offering consumers notice of the sale and providing an opportunity to Opt-in[14] or Opt-out of having their personal and financial records transferred to the Purchaser.[15]

---

[12] The State Attorneys General objected to the sale, arguing that because sensitive records about children and credit card numbers were being sold, consumers should be permitted to consent to the sale through an Opt-In procedure. Because the records were not sold within a specified period of time, they were destroyed. Objection of the Commonwealth of Massachusetts and 46 States to the Debtor's Motion to Approve Settlement with Federal Trade Commission and for Authority to Enter in Consent Agreement, page 8. *In re* Toysmart.com LLC, No. 00-13995-CJK (U.S. Bankr. Court, D. Mass.), ["*In re* Toysmart.com"] *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/x000075-toysmartcom-llc-toysmartcom-inc.

[13] *In re* Borders Group, Inc., No. 11-10614-mg (Bankr. S.D.N.Y.) (Glenn, J.), *In re* RadioShack Corporation, No. 15-10197 (BLS) (Bankr. D. Del.) (Shannon, J.); *In re* Choxi, 16-13131 (SCC) (Bankr. S.D.N.Y.) (Chapman, J.); *In re* Century 21 Department Stores, 20-12097 (Bankr. S.D.N.Y.) (Chapman, J.); *In re* KB US Holding 20-22962 (SHL) (Bankr. S.D.N.Y.) (Lane, J); *In re* MKJC Hyundai, 20-42283, (Bankr. S.D.N.Y.) (Mazer-Marino, J.); *In re* Loot Crate, 19-11791-BLS (Bankr. D. DE) (Shannon, J.); *In re* NovaSom, 19-11734 (BLS) (Bankr. D. DE) (Shannon, J.); *In re* Hobbico, 18-10055 (KG) (Bankr. D. DE) (Gross J.); *In re* Circuit City Stores, 3:08-bk-35653 (Bankr. E.D. VA) (Huennekens, J.); *In re* Linens N Things, 08-10832 (CSS) (Bankr. D. DE) (Sontchi, J.).

[14] The determination of whether an Opt-in or an Opt-out process should be followed is based on data sensitivity; an Opt-in process is usually appropriate for the sale of the most sensitive consumer data.[14] *In re* Toysmart.com, *supra* note 12.

[15] This approach is consistent with FTC recommendations in prior bankruptcy cases to limit the amount of data in the sales. For example, in the Borders bankruptcy case, the FTC recommended that any transfer of personal information take place only with the consent of Border's customers or with significant restrictions on the transfer and use of the information. *In re* Borders Group, Inc., No. 11-10614-mg (Bankr. S.D.N.Y.) (Glenn, J.) FTC Seeks Protection for Personal Customer Information in Borders Bankruptcy Proceeding, (Sep. 21, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/09/ftc-seeks-protection-personal-customer-information-borders-bankruptcy-proceeding.

Those records not sold included data about children,[16] financial data (credit card numbers and bank and tax records),[17] dating site records of encounters and personal communications,[18] records of books and videos purchased,[19] subscribers to XY, a gay male youth-oriented magazine, including photos and online profiles,[20] demographic data (racial/ethnic, age, children, household members' income and education),[21] patient healthcare records,[22] medical records[23] and genetic data,[24] details of retail transactions,[25] and multiple copies of personal data on backup media.[26]

Decisions to limit the sale of certain personal data were based on and reflect the well-accepted privacy principles – Fair Information Practice Principles (FIPPs) – which are fundamental to privacy laws today.[27] The FIPPs consist of eight privacy principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. The data

---

[16] *In re* Toysmart, *supra* note 12.

[17] Numerous cases, including *In re* JK Harris & Co. No. 2:11-bk-06254 (Bankr. D. SC) (Waites, J.).

[18] *In re* True Beginnings, No. 4:12-bk-42061 (ED TX) (Rhoades, J.)

[19] *In re* Borders Group, Inc., *supra* note 15.

[20] *In re* Peter Ian Cummings, Case No. 10-14433 (Bankr. D. N.J.) (Kaplan, J.) An FTC letter requested that the data be destroyed, suggesting the sale could violation the FTC Act prohibition against unfair or deceptive acts or practices. https://www.ftc.gov/system/files/documents/closing_letters/letter-xy-magazine-xy.com-regarding-use-sale-or-transfer-personal-information-obtained-during-bankruptcy-proceeding/100712xy.pdf.

[21] *In re* QSL of Medina, No. 15-52722 (Bankr. ND NY) (Koschik, J.)

[22] *In re* NovaSom, No. 19-11734 (BLS) (Bankr. D DE) (Shannon, J.)

[23] *In re* Laboratory Partners, No. 1:13-bk-12769 (Bankr. D.Del.) (Silverstein, J.)

[24] *In re* deCODE Genetics, No. 09-14063 (Bankr. D.Del.) (Silverstein, J.)

[25] *In re* Circuit City, No. 3:08-bk-35653 (Bankr. E.D.Va.) (Huennekens, J.)

[26] *In re* Linens N Things, 08-10832 (CSS) (D DE) (Sontchi, J.)

[27] The FIPPs principles are found in the Organization for Economic Cooperation and Development (OECD) Privacy Principles, which have been incorporated in the European Union (EU) General Data Protection Regulation (GDPR), by the American Institute of CPAs (AICPA) in adopting its Generally Accepted Privacy Principles, and by the U.S. Department of Commerce Safe Harbor and Privacy Shield Programs. OECD Privacy Principles, http://oecdprivacy.org/#version; EU-US Privacy Shield Framework Principles Issued by the U.S. Department of Commerce, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg. *Supra* note 4.

included in the sale should be limited to the "minimum necessary" to achieve the Purchaser's business objectives. Information excluded from the sale should be maintained in accordance with legal requirements reflected in an appropriate data retention schedule.

The heightened risk of data breaches of the Celsius account holders data should also be a paramount concern, because crypto companies have been targeted by hackers. Minimizing the amount of personal data collected, maintained, and sold by companies is one of the most effective ways to protect it from data breaches. The massive databases of personal and financial data that have been created and maintained by companies have become the target of cyber attacks by nation states, hackers, and criminal groups.[28] Law enforcement has documented the heightened risks of cyber breaches throughout the crypto ecosystem. In the past few years, these breaches have occurred with alarming frequency. Millions of personal and financial records have been stolen and huge losses to the companies and their investors have resulted. If consumer data falls into the wrong hands, there is a vibrant black market for stolen personal data, often posted on the dark web, and the risk of identity theft and fraud has increased dramatically.[29]

B. Recommendations – Essential Privacy Issues to Address; Practical Steps

At the January 24, 2023 hearing, the Debtors presented a proposal for an "asset recovery plan." In lieu of an outright sale to a third party and/or a potential competitor, the Debtors are developing a plan for the creation of a new public corporation with professional management.

[28] The Honorable Avril Haines, Dir. of Nat'l Intelligence, Statement for the Record to the Senate Select Comm. on Intelligence, Annual Threat Assessment of the U.S. Intelligence Community (April. 29, 2021), page 20, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf. ("Cyber threats from nation states and their surrogates will remain acute. Foreign states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure."); FBI The Cyber Threat, https://www.fbi.gov/investigate/cyber.

[29] National Council on Identity Theft Protection, *2023 Identity Theft Facts and Statistics*, https://identitytheft.org/statistics/. (The frequency of identity theft "has sky-rocketed in the past few years. We aren't finished with the year 2023, but the statistics for identity theft are already quite alarming.")

Through a "recovery corporation," the value of the Debtors' assets, including the Debtors' liquid and illiquid cryptocurrency, loan receivables, mining assets, and proceeds from litigation claims, would be distributed to account holders. [ECF No. 1940, filed 1/26/23]

Thus, the recommendations that follow are tentative and subject to change based on the Debtors' final plans for what account holder data may be sold or transferred to the new corporation.

1. Debtors' Plans: May Not Include Inactive Accounts in the Sale or Transfer

The Ombudsman has been advised that the Debtors do not plan to sell the data of individuals with inactive accounts. She was also told that one potential Purchaser, if a sale to a third party is contemplated, has indicated an interest in buying only the data of account holders who reside in the U.S. Data of non-U.S. based investors would not be sold.

If the data concerning individuals with inactive accounts is not sold, that decision will protect the privacy of more than one million Celsius account holders.

***Next steps*:** Protection of data throughout its entire lifecycle is important when volumes of sensitive personal data have been collected and maintained by Celsius. To protect confidential information, an organization must know what data it has, where it resides, its level of sensitivity, and how it is secured. The data collected and maintained by Celsius (stored in all locations on servers, mobile devices, in the cloud, on backup cloud/media storage, etc.) should be catalogued and its sensitivity evaluated. The Ombudsman has been advised that these tasks have been addressed by Celsius and its systems, policies and processes have been externally audited.

Celsius has received certifications for both Information and Security Management (ISO 27001) and Privacy Information Management (ISO 27001).

The Ombudsman is available to assist in developing an appropriate plan for data retention, disposition, and disposal of all the personal and financial data that will not be sold. Decisions should be made in accordance with applicable laws and FTC rules, the Bank Secrecy Act, Know Your Customer (KYC), IRS and other federal data retention requirements, state data disposal laws, and GDPR and country laws.[30]

2. Proposed Sale or Transfer of Current Account Holder Data

***Next steps*:** When details of the Debtors' "asset recovery plan" are finalized, they should inform the Court and the Ombudsman of what account holder data the company plans to sell or transfer to a new entity. The Ombudsman proposes to work with the Debtors to help identify and define the privacy and security measures to be adopted.

- Apply the "Qualified Buyer" criteria for the proposed Purchaser/ New Company. (Section V.A. *infra, page 37*.)
- Develop an appropriate privacy policy for the new company that reflects the legitimate interests of the company and protects the privacy of account holders' data.
- Conduct due diligence: Celsius should evaluate the proposed Purchaser/ New Company according to the Celsius third party due diligence "checklist" (January 2022).

[30] Celsius Terms of Use, 3. Eligibility and Proof of Identity: Celsius is subject to AML, KYC, and U.S. sanction requirements under the Bank Secrecy Act (**"**BSA**"**), Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act"), and the Office of Foreign Assets Control ("OFAC**"**). Passport and driver's license are among the information collected.

Under applicable Anti-money Laundering (AML) and OFAC rules, Celsius is obligated to maintain certain information about you, including User records and transaction history, for five years (seven years for Users residing in the state of New York), or a longer period as may be required under applicable laws.

Ensure the proposed CEO and officers and directors or third party plan sponsor have developed and implemented a comprehensive cybersecurity program, conducted a risk assessment, and is in compliance with the Safeguards and Red Flags Rules.

- Define a targeted sale that includes only the "minimum necessary" personal and financial data of current account holders.
- Evaluate the sensitivity of the data. Review and segregate data that does not need to be sold and cannot be justified as necessary for the legitimate business purposes of the proposed Purchaser/ New Company. A core privacy principle ("purpose limitation") requires that the purpose for collection of the information must be specified and the data cannot be used for a different purpose unless the user consents or it is required by law.
- Develop a plan for notification of current account holders regarding the benefits of the migration of their accounts to the platform of the proposed Purchaser or the New Company; obtain consent.

  During the Chapter 11 Plan approval process, account holders will be provided notice and adequate time to make an informed decision on whether to vote to approve the plan. The current plan is to solicit votes through June 30, 2023. [ECF No. 1940, filed 1/26/23]

In many prior bankruptcy cases, the parties adopted an Opt-out process designed to protect the privacy of all consumers to the greatest extent possible under the circumstances of this bankruptcy sale. The goal was to ensure that the process was transparent, meaningful and effective. Notice was provided to all consumers with a clear and conspicuous notice on the new Purchaser's website of the change of corporate ownership and management of their right to Opt-out of the transfer of their personal information to the Purchaser. Further notice to customers was

provided by e-mail. The Celsius App may provide a mechanism for an effective notice. The process should be incorporated in the Sale Order.

- Develop a notice and Opt-in/ Opt-out process for California residents as required by the Celsius privacy policy: "California Resident's Rights Under the CCPA." "We do not sell your personal information." If your personal information is subject to the CCPA, you may have certain rights with regard to such personal information, including the right to: Opt-Out of Sale. Request that we not sell your personal information if a business sells your personal information (we do not)."

Virginia has a new privacy law (Colorado and Connecticut laws become effective in July 2023) that may also require an Opt-out process for the sale. 64,817 (27 percent) reside in those four states.

- Review GDPR requirements and country laws that may require special data disposition processes (required by the Celsius privacy policy). Of the total active Celsius account holders, 366,772 individuals reside outside the U.S. in 210 countries around the world.
- Develop an Opt-out process as required by the Celsius privacy policy for residents of the EU countries covered by the GDPR. More than 150,000 Celsius users are located in the 27 EU countries.
- Develop an appropriate plan for data retention, disposition and disposal of all data of individuals not sold in accordance with applicable laws (*e.g*. California, GDPR, etc.) and FTC rules, Bank Secrecy Act, Know Your Customer (KYC), IRS and other federal data retention requirements, state data disposal laws, and GDPR and country laws. Specific plans must be developed for the more than 350,000 individuals whose data must be protected by the GDPR and applicable country laws.

II. Factual Background

A. Celsius Bankruptcy

On July 13, 2022 Celsius Network LLC and related businesses ("Debtors") filed voluntary petitions under chapter 11 of the Bankruptcy Code. The Debtors are operating their business and managing their property as debtors-in-possession.

The Debtors' corporate headquarters is located in Hoboken, New Jersey. The company maintains a website at https://celsius.network/. Celsius Network LLC is a Delaware Limited Liability Company. The Terms of Use specify that the relationship between users and Celsius is governed by the laws of the state of New York.[31]

Celsius was created in 2017 and provided financial services to institutional, corporate, and retail clients across more than 100 countries. Celsius' primary operations consisted of: (a) financial services through which retail and institutional users can (i) earn rewards on cryptocurrency they transferred to Celsius, (ii) securely store and access cryptocurrency, (iii) borrow fiat[32] using cryptocurrency as collateral, and (iv) send and receive cryptocurrency using Celsius' CelPay services; and (b) Bitcoin mining through Mining. Mashinsky Declaration I, ¶ 42. [ECF No. 23, filed 7/14/22] [33]

[31] The most recent version of the Terms of Use dated September 29, 2022 is posted on the Celsius website at https://celsius.network/terms-of-use. Its stated terms are applicable beginning on April 15, 2022 and "govern each User's access to, and use of, Celsius' products and services."

[32] Celsius Terms of Use, 2. Definitions. "Fiat," when used in reference to money or currency, means the coin and paper money of a country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance.

[33] A detailed description of the Celsius cases is set forth in the Declaration of Robert Campagna, Managing Director of Alvarez & Marsal North America, LLC, in Support of Chapter 11 Petitions and First Day Motions. [ECF No. 22, filed 7/14/22]. Further details of the company's operations are provided in the Mashinsky Declarations I and II [ECF No. 23, filed 7/14/22; ECF No. 393, filed 8/8/22], *supra* note 10. The Interim Report of the Examiner describes the Debtors' cryptocurrency holdings [ECF No. 1411, filed 11/19/22].

Users accessed the Company's entire suite of services through Celsius' web or mobile application (collectively, the "Celsius App"). Users signed up for a Celsius account on the Celsius App and were asked to digitally execute Celsius' user agreement and "Terms of Use" before being permitted to use the platform to facilitate the purchase or transfer of cryptocurrency. Mashinsky Declaration I, ¶ 60.

In 2022 Celsius advised the Court that in an effort to "stabilize its business and protect its users," on June 12, 2022 the company decided to pause all withdrawals, swaps, and transfers on its platform. This "pause" was intended to prevent certain users—those who were the first to act—from being paid in full while leaving other users behind to wait for Celsius to harvest value from illiquid or longer-term asset deployment activities before they received a recovery. Mashinsky Declaration I, ¶ 14.

B. Request to Sell Celsius Retail Platform Assets

The Debtors obtained Bankruptcy Court approval to conduct a sale process for the sale of their "Retail Platform Assets" (as defined in the Bidding Procedures). The Court entered an Order on November 2, 2022 approving the bid procedures and auction process. ("Bidding Procedures Order")[34] [ECF No. 1272, filed 11/2/22].

The Order states that the "Retail Platform Assets" include "customer earn accounts and coin balances, retail and institutional lending portfolio, swap services, staking platform, CelPay (the Debtors' cryptocurrency payment and transfer feature), and CelsiusX (the Debtors' decentralized finance arm that utilizes wrapped cryptocurrency tokens to bridge centralized finance infrastructure to decentralized finance opportunities), and any cryptocurrencies or digital

[34] Order (I) Approving the Bidding Procedures in Connection With the Sale of Substantially All of the Debtors' Assets, (II) Scheduling Certain Dates With Respect Thereto, (III) Approving the Form and Manner of Notice Thereof, (IV) Approving Contract Assumption and Assignment Procedures, and (V) Granting Related Relief. [ECF No. 1272, filed 11/2/22].

assets held by the Debtors (to the extent that they comprise property of the estate as such term is defined under section 541of the Bankruptcy Code)." The Debtors are evaluating whether the value of the estates would be maximized through a stand-alone restructuring or a sale of some or all of the Assets. Bidding Procedures Order, pages 2-4.

C. Proposed Purchaser(s)

The Bidding Procedures Order authorized the Debtors to enter into an Asset Purchase Agreement ("APA") prior to the sale between the proposed Purchaser and the Debtors. The Debtors have actively pursued a dual-track process of marketing all of their assets for sale while simultaneously developing a path towards a standalone reorganization. In lieu of an outright sale to a third party and/or a potential competitor, the Debtors are currently developing an "asset recovery plan" for the creation of a new public corporation.

A hearing to discuss the "asset recovery plan" is scheduled before the Court on February 15, 2023.[35] [ECF No. 1844, filed 1/9/23].

III. Celsius Terms of Use and the Privacy Policy

Celsius published a privacy policy on its website (last revised October 2021). It was in effect on the bankruptcy petition date. (The most recent Celsius privacy policy is attached to this CPO Report as Appendix A). Between February 1, 2018 and April 14, 2022, the Debtors published eight versions of its Terms of Use governing the use of the Debtors' platform.[36] Several of the Terms of Use reference: (a) the Celsius Privacy Policy (the "Privacy Policy"), which outlines the Debtors' practices with respect to collecting, using, and disclosing customer

[35] Second Notice of Amended Dates and Deadlines With Respect to Bidding Procedures for the Potential Sale of Substantially All of the Debtors' Assets [ECF No. 1844, filed 1/9/23].

[36] Details of the Celsius Terms of Use are set forth in the Declaration of Alex Mashinsky, Chief Executive Officer of Celsius Network LLC, providing terms of use dating back to February 18, 2018 [ECF No. 393, filed 8/08/22] Privacy Policy at Exhibit H, Pg. 1072 of 1126. ["Mashinsky II"], *supra* note 34.

information; and (b) the Celsius Risk Disclosure (the "Risk Disclosure"), which outlines the risks involved in holding, trading, and using digital assets generally, as well as the use of the services offered by the Debtors.

This CPO Report highlights sections of the privacy policy that identify the personal data collected and maintained by Celsius and the company's data sharing policies and are pertinent to the analysis of and potential privacy risks in connection with the sale of the personal consumer information.

The privacy policy provides, in pertinent part (excerpts):

> Celsius Network LLC… respects the privacy of our users… and is committed to protecting the privacy of Users who access, download, install or register to our mobile or web application…, our website or any other online services we provide (collectively: the "Services").
>
> The information we request from you will be the minimum required to provide you with our services.
>
> **What Type of Information We Collect**
>
> When we use the term "Personal Information" we mean any information about an individual from which that person can be identified. Information that is anonymous, aggregated, or deidentified is generally not considered Personal Information.
>
> There are instances where we invite or request individuals to provide us with their Personal Information through our Application, website or otherwise (e.g. by email), and we may also collect some information automatically. Through your use of our Services and your interactions with us, you may provide us with Personal Information including:
>
> - **Identifiers and similar information** such as, name, address, date of birth, email address, social security number, driver's license number, passport number, online identifiers, or other similar identifiers;
> - **Certain information protected under federal or state laws** such as a signature or bank account or other financial information;
> - **Characteristics of protected classifications** under certain federal or state laws, including gender, national origin, or marital status;
> - **Commercial information**, including records of products or services purchased, obtained, or considered, or other purchasing histories or tendencies;
> - **Internet or other electronic network activity information**, including interactions with our website or use of certain online tools;

- **Geolocation data**, such as information about your location or the location of your device;
- **Audio, electronic, visual**, or similar information, which could be collected during audio or video calls (including video conferences and similar functions);
- **Biometric data**, such as images, which may constitute biometric data in certain jurisdictions. We may use such data for the purpose of identification for fraud and anti-money laundering checks;
- **Professional or employment-related information**, including occupation, compensation, employer, and title;
- **Inferences drawn from any of the information identified above** to create a profile reflecting your preferences or similar information[.]

Sources of Personal Information

- We collect Personal Information about you directly from you and/or your intermediaries through sources on our website, our Application, when you register or sign-in to the Services via your social network account, including when the following happens:
- **Signing up for an account**: When you sign-up and register for the Services, you will be asked to provide us certain details about yourself. You may register for the Services through your social network account or directly through the Application or our website (if applicable).
- **Registering through social network account**: When you register or sign-in to the Services via your social network account (e.g., Facebook, Twitter, etc.), we will have access to basic information from your social network account, such as your full name, home address, email address, birthdate, profile picture, friends list, personal description, as well as any other information you made publicly available on such account or agreed to share with us. At all times, we will abide by the terms, conditions and restrictions of the social network platform.
- **Voluntarily provided information**: … communications to and from us, and feedback, suggestions, complaints and reports which you send to us. Please note that we may also collect complaints about you from other Users, which may include your Personal Information.
- **Communication Recording**: We may record communications between you and any of our representatives and/or other participants, including recordings of audio, video and video conference calls, conversations or communications. We may collect this information for the purpose of resolving complaints, or for the purpose of improving the overall quality of the Services, for training and/or instructional purposes, record keeping or otherwise in order to comply with a legal or regulatory requirement to which we are subject.
- **Device information**: … Such information may include geolocation data, IP address, unique identifiers (e.g., MAC address and UUID) as well as other information which relates to your activity through the Services.

In addition, we may collect Personal Information from different sources, such as:

[O]ur affiliates, our service providers, or our affiliates' service providers; public websites or other publicly accessible directories and sources, including bankruptcy registers, tax authorities, governmental agencies and departments, and regulatory authorities; and/or

from credit reporting agencies, sanctions screening databases, or from sources designed to detect and prevent fraud or financial crimes. The relevant source may be responsible for obtaining the relevant consents from you (where applicable) to ensure you are happy with the ways in which your Personal Information will be used.

Cookies and Google Analytics

We may use cookies and other technologies or methods of web and mobile analysis to gather, store, and track certain information related with your access to and activity through the Services, including when you visit our website.

With Whom We Share the Information and for What Purpose

- We do not rent, sell, or share your Personal Information with third-parties except as described in this Privacy Policy.
- We may share Personal Information with the following recipients: (i) our subsidiaries; (ii) affiliated companies; (iii) subcontractors and other third-party service providers; (iv) business partners (such as GEM, Coinify, Simplex and Wyre); (v) auditors or advisers of our business processes; and (vi) any potential purchasers or third party acquirer(s) of all or any portion of our business or assets, or investors in the company.

  In addition to the purposes listed in this Privacy Policy, we may share Personal Information with our recipients for any of the following purposes: (i) storing or processing Personal Information on our behalf (e.g., cloud computing service providers); (ii) processing such information to assist us with our business operations; (iii) carrying out your instructions or giving effect to your preferences in relation to the Services we provide (including if you wish to use services which our business partners provide); (iv) performing research, technical diagnostics, personalization and analytics.

  We may also disclose Personal Information or any information we may have about you if we have a good faith belief that disclosure of such information is helpful or reasonably necessary to: (i) comply with any applicable law, regulation, legal process or governmental request; (ii) enforce our policies, including investigations of potential violations thereof; (iii) investigate, detect, prevent, or take action regarding illegal activities or other wrongdoing, suspected fraud or security issues; (iv) to establish or exercise our rights to defend against legal claims; (v) prevent harm to the rights, property or safety of us, our affiliates, our Users, yourself or any third-party; (vi) for the purpose of collaborating with law enforcement agencies; and (vii) in case we find it necessary in order to enforce intellectual property or other legal rights.

  Wherever possible, we will only disclose Personal Information to a third party in circumstances where that third party has agreed to respect the security and confidentiality of Personal Information and treat it in accordance with applicable law. We will seek to ensure that third parties to whom any Personal Information may be disclosed will not use Personal Information for their own purposes and only process Personal Information for

specified purposes and otherwise in accordance with our instructions and/or with applicable laws.

Corporate Transactions

We may share information, including Personal Information, in the event of a corporate transaction (e.g., sale of a substantial part of our business, merger, consolidation or asset sale of an asset or transfer in the operation thereof) of the Company. In the event of the above, the acquiring company or transferee will assume the rights and obligations as described in this Privacy Policy.

For How Long We Retain Your Information

How long we keep your Personal Information will vary depending on the type of Personal Information and our reasons for collecting it. The retention period will be determined by various criteria, including the purposes for which we are using it (as it will need to be kept for as long as is necessary for any of those purposes) and our legal obligations (as laws or regulations may set a minimum period for which we have to keep your Personal Information). In general, we will retain your Personal Information for as long as we require it to perform our contractual rights and obligations, resolve disputes and enforce our policies and agreements, or for periods required by our legal and regulatory obligations.

How We Protect Your Information

We take great care in implementing and maintaining the security of the Services and your information. We will take reasonable steps and use technical, administrative and physical security measures appropriate to the nature of the information and that comply with applicable laws to protect Personal Information against unauthorized access and exfiltration, acquisition, theft, or disclosure. Although we take enhanced steps to safeguard information, given the nature of information security, there is no guarantee that such measures will always be successful. We cannot be responsible for the acts of those who gain unauthorized access or abuse the Services, and we make no warranty, express, implied or otherwise, that such access will be prevented. If you feel that your privacy was treated not in accordance with our policy, or if any person attempted to abuse the Services or acted in an inappropriate manner, please contact us directly at info@celsius.network.

EU/UK Based Users and the GDPR

If you are an EU or UK data subject and the processing of your Personal Information is subject to the GDPR, please review this section in addition to the entire Policy.

Additional Information for California Residents
Our Disclosure, Sharing of Personal Information

We do not sell your personal information.

California Resident's Rights Under the CCPA

If your personal information is subject to the CCPA, you may have certain rights with regard to such personal information, including the right to:

Opt-Out of Sale. Request that we not sell your personal information if a business sells your personal information (we do not).

The **Terms of Use** reference other information collected by Celsius:

- Virtual Wallet IDs
- Designated withdrawal addresses in user profiles (for digital assets Celsius returns to users)
- Information, including passport and driver's license numbers, collected to comply with the AML, KYC, BSA, USA PATRIOT Act, and OFAC requirements. *Supra* note 29.
- Section 29. Communications. We may record and monitor our telephone conversations with you and your electronic communications with us (chat, email, and other forms of electronic exchange).

IV. Potential Gains and Losses to Celsius Consumers if the Sale or Transfer is Approved

A. Potential Gains of Privacy or Benefits to Consumers

As referenced earlier, the Debtors are working on an "asset recovery plan" that, within the constraints of this bankruptcy case, could provide tangible benefits for the investors with active accounts. The goal is to "harvest[] the value of the Debtors' illiquid assets over time and distribute[] that value to account holders."

Thus, it is too early to know specifically what gains of privacy or benefits to consumers will result from the sale or transfer to a new entity. Creation of a "recovery company" would provide an excellent opportunity for the entity to adopt a new privacy policy that reflects its legitimate business interests while providing privacy protections for the account holders. The Ombudsman will work with the parties to help develop appropriate privacy protections when further information about the new company is available.

1. Active Account Holders

Based on data provided to the Ombudsman and the account records of individual retail customers published in the Statement of Financial Affairs and Schedules, Celsius has more than 600,000 active account holders. [ECF No. 974, filed 10/5/22].

At the December 20, 2022 status conference, the Debtors presented the testimony of Christopher Ferraro who advised that the Debtors have received multiple bids proposing a range of potential transaction and business structures to acquire the retail platform assets and provide value to the Debtors' estates. The Debtors are also working on plans for a standalone reorganization of the company. Ferraro Presentation 12/20/22 [ECF No. 1758, filed 12/19/22].

The following options presented by Mr. Ferraro include references to potential benefits to users whose accounts are migrated to the new platform. In addition to any financial benefits, privacy protections should be specified.

	Sale of Celsius Retail Platform Assets Potential Structures
Customer Migration	• The acquiror will pay the Debtors' estates to migrate customer accounts and the Debtors' crypto assets to the acquiror's platform. • Customers will receive access to a percentage of the Debtors' crypto assets on the acquiror's platform.
Asset Management Platform	• The Debtors' assets will be transferred to a newly formed asset management entity managed by the acquirors. • The Debtors' creditors will receive crypto tokens representing the value of assets and business operations in the newly formed entity, which will trade on the blockchain, as well as tokens representing a portion of the management fee paid to the asset manager.
Distribution Services	• The Debtors' assets will be transferred to the acquiror's platform. • The Debtors' creditors will receive access to a pro rata portion of the Debtors' crypto assets through the acquiror's platform. • Illiquid assets transferred to special purpose vehicles with equity in the acquiror's platform distributed to creditors.
	ECF No. 1758, filed 12/20/22

Asset Recovery Plan

In lieu of an outright sale to a third party and/or a potential competitor, the Debtors are developing a plan for the creation of a new public corporation with professional management.

Through a "recovery corporation," the value of the Debtors' assets, including the Debtors' liquid and illiquid cryptocurrency, loan receivables, mining assets, and proceeds from litigation claims, would be distributed to account holders. [ECF No. 1940, filed 1/26/23]

As presented at the January 24, 2023 omnibus hearing, discussions are crystalizing around a framework with the following key features:

- ***Recovery Corporation Features***. The Debtors are considering operating the recovery corporation on a stand-alone basis or via a third party plan sponsor who would invest in and operate the recovery corporation. In either formulation, the recovery corporation will be fully licensed and registered[37] and will comply with all applicable federal and state regulations. The recovery corporation will also have a dedicated management team and digital assets will be held by a licensed third-party custodian. Discussions regarding the mining assets remain ongoing.

- ***Form of Consideration for Creditors***. The interests of the recovery corporation will be "tokenized" and distributed to account holders with claims above a certain threshold as "Asset Share Tokens" that reflect the value of the assets managed by the recovery corporation. Asset Share Tokens will entitle their holders to dividends from the recovery corporation as assets are monetized and will be freely tradeable by holders.

- ***Convenience Class.*** All creditors with claims under a certain threshold, or creditors who choose to reduce their claims to the threshold, will be offered a one-time distribution of liquid cryptocurrency (*e.g.*, stablecoins, Bitcoin, or Ethereum) at a discount to the value of their claims.

- ***Establishment of a Litigation Trust***. The Debtors also expect to create a litigation trust to pursue claims against certain insiders, claims identified in the Examiner's report, as well as other claims and causes of action that will be agreed upon by the Debtors and the Committee.

Once negotiations are completed and the documentation is finalized, the Debtors anticipate promptly filing a chapter 11 plan reflecting the value-maximizing path forward.

---

[37] As discussed in section VI.A. of this CPO Report, regulators regulate financial institutions, markets, and products using licensing, registration, rulemaking, supervisory, enforcement, and resolution powers. In practice, regulatory jurisdiction is typically based on charter type, not function. In other words, how and by whom a firm is regulated depends more on the firm's legal status than the types of activities it is conducting.

The regulatory framework for cryptocurrencies is evolving despite overlap and differences in viewpoints between agencies. The SEC often views many cryptos as securities, the CFTC calls bitcoin a commodity, and Treasury calls it a currency.

2. Celsius Users with Inactive Accounts

The Debtors have collected personal and financial data on more than one million individuals whose Celsius accounts are inactive. The Debtors have advised the Ombudsman they do not plan to sell the data of individuals with inactive accounts. In keeping with that decision, the "asset recovery plan" proposed for the retail platform assets does not address the sale of inactive accounts.

The Ombudsman supports that decision and agrees that absent a compelling justification, the personal and financial data of investors with inactive accounts should be excluded from the sale or transfer to a new entity. *If the data concerning individuals with inactive accounts is not sold, that decision will protect the privacy of more than one million Celsius account holders*.

If some of the consumer data is sold or transferred, recommended privacy protections are set forth in Section V. of this CPO Report. If all the personal and financial data for individuals with inactive accounts is excluded from the sale or transfer, a data retention plan and a protocol for destruction of the data in compliance with state data disposal laws, as well as country privacy laws, must be developed.

B. Potential Losses of Privacy or Costs to Consumers if the Sale/Transfer is Approved

A review of the Celsius privacy policy reveals that the company collected some of the most highly sensitive data available, including not only personally identifiable information, but also protected demographic classifications, geolocation and biometric data, and information protected under federal and state laws.[38] Bankruptcy courts did not permit some of these types of data to be sold in prior cases (discussed *supra* at footnotes 13-24.).

[38] ***Identifiers*** and similar information; Certain ***information protected under federal or state laws*** such as a signature or bank account or other financial information; ***Characteristics of protected classifications*** under certain federal or state laws, including gender, national origin, or marital status; ***Commercial information***; ***Internet or other electronic network activity information***; ***Geolocation data***; ***Audio, electronic, visual, or similar information***;

With the development of databases containing vast amounts of sensitive personal and financial information, much is at stake in the potential sacrifice of personal privacy with a sale of the Celsius account holder data. With ever more sophisticated technical capabilities for data aggregation and data mining, coupled with powerful business intelligence and analysis tools, the privacy of individuals could be jeopardized. The FTC has recently reported on the risks of the use and sharing of highly sensitive consumer data, such as geolocation data and healthcare records.[39]

1. U.S. Assessment of Opportunities and Risks with Digital Assets

Current White House initiatives have focused on consumer and investor protection, among other issues, in the cryptocurrency arena. In light of unprecedented warnings from the FBI concerning the potential exposure of cryptocurrency customer account information to cybersecurity risks, the Court should engage in its own careful scrutiny of the sensitive personal and financial data to be sold – limiting it to only the information justified as necessary for the legitimate business purposes of the proposed Purchaser.

Executive Order (EO) 14067 on Ensuring Responsible Development of Digital Assets (2022) addressed the risks and potential benefits of digital assets and identified six key priorities the U.S. should pursue: consumer and investor protection; promoting financial stability;

Biometric data; ***Professional or employment-related information***; ***Inferences*** drawn from any of the information identified above to create a profile reflecting your preferences or similar information[.]

[39] Kristin Cohen, FTC Business Blog, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data* (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

("Among the most sensitive categories of data collected by connected devices are a person's precise location and information about their health." "Standing alone, these data points may pose an incalculable risk to personal privacy. Now consider the unprecedented intrusion when these connected devices and technology companies collect that data, combine it, and sell or monetize it. This isn't the stuff of dystopian fiction. It's a question consumers are asking right now.")

countering illicit finance; U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation.[40]

On September 16, 2022, the White House released a report on "Protecting Consumers, Investors, and Businesses"[41] that made the following observations:

> Digital assets pose meaningful risks for consumers, investors, and businesses. Prices of these assets can be highly volatile: the current global market capitalization of cryptocurrencies is approximately one-third of its November 2021 peak. Still sellers commonly mislead consumers about digital assets' features and expected returns, and non-compliance with applicable laws and regulations remains widespread. One study found that almost a quarter of digital coin offerings had disclosure or transparency problems—like plagiarized documents or false promises of guaranteed returns.[42] Outright fraud, scams, and theft in digital asset markets are on the rise: according to FBI statistics, reported monetary losses from digital asset scams were nearly 600 percent higher in 2021 than the year before.

The White House report emphasized the importance of "[d]eveloping, designing, and implementing digital assets in a responsible manner that includes privacy and security in their architecture, integrating features and controls that defend against illicit exploitation, and reducing negative climate impacts and environmental pollution."

As discussed earlier in this CPO Report, the January 3, 2023 *Joint Statement on Crypto-Asset Risks to Banking Organizations* by the three leading federal banking agencies observed that the "events of the past year have been marked by significant volatility and the exposure of

---

[40] The White House, Executive Order on Ensuring Responsible Development of Digital Assets (March 9, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/. ["EO 14067"]

Over the past six months, federal agencies submitted nine reports that articulate a clear framework and policy recommendations for responsible digital asset development. They reflect the expertise of diverse stakeholders across government, industry, academia, and civil society.

[41] Fact Sheet: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets (Sep. 16, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/.

[42] Shane Shifflet and Coulter Jones, *Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud: A Wall Street Journal analysis of 1,450 cryptocurrency offerings reveals rampant plagiarism, identity theft and promises of improbable returns* (May 17, 2018), https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115.

vulnerabilities in the crypto-asset sector."[43] The statement highlights eight crypto-asset risks, many of which affected and may have harmed retail investors and customers.

The 1.7 million Celsius current and former account holders may have experienced some of the harms identified by the experts and presented in the White House and banking regulators' reports. Some individuals have lost all or part of their investments. The Celsius bankruptcy case docket is filled with letters to the Court and investor claims for substantial losses, each describing his/her own unique circumstances. Using its discretion to require appropriate privacy protections for the sale, the Court can ensure that from this point forward, the privacy of the Celsius account holders will be protected.

2. Celsius Privacy Policy Tilts the Balance Toward the Company

The Celsius privacy policy tips the balance of power toward promoting Celsius business interests and away from protecting the privacy of individuals. While the purpose of a privacy policy is to advise consumers of the information practices of the company, in recent years companies have published expansive policies authorizing very broad data collection and sharing practices. As discussed above, creation of the "recovery corporation" will provide an opportunity to develop a new privacy policy that reflects the legitimate interests of the company and protects the privacy of account holders' data.

The Celsius privacy policy is drafted so that company officials – not individual investors – will make important, unilateral determinations about the privacy protections to be provided for the personal data of Celsius users. A recent FTC study focused on Internet Service Providers

[43] Banking Regulators Joint Statement, *supra* note 7.

(ISPs) illustrates the widespread use of these types of broad privacy policies by technology companies and how they can be harmful to consumers.[44]

The issues identified by the FTC report and the resulting harm to consumers should be recognized in evaluating what privacy protections are appropriate to apply in the proposed sale or transfer of the account holders data in this case. The FTC criticized many of the same features of corporate privacy policies as are contained in Celsius' privacy policy, *e.g.*, provisions promising privacy protections with exceptions and authorizations for widespread sharing, unfettered discretion to gather personal data absent business need, and lack of accountability.

The Celsius privacy policy makes explicit promises that could be interpreted as sending mixed messages to account holders – promising a strong commitment to privacy – while as the same time taking away genuine privacy protections with a multitude of authorizations and exceptions.

> Celsius Network LLC… respects the privacy of our users… and is committed to protecting the privacy of Users who access, download, install or register to our mobile or web application…, our website or any other online services we provide (collectively: the "Services").
>
> The information we request from you will be the minimum required to provide you with our services.
>
> We do not rent, sell, or share your Personal Information with third-parties except as described in this Privacy Policy.

The privacy policy permits or authorizes the company to collect, use, share, and sell some of the most highly sensitive data available, including not only personally identifiable information, but also protected demographic classifications, geolocation and biometric data, and

[44] FTC, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf. ("Although many ISPs purport to offer consumers choices, these choices are often illusory.") ["FTC Privacy Practices Report"]

information protected under federal or state laws[45] for marketing, profiling and advertising, as well as conducting financial transactions. As the FTC report observed, many corporate privacy policies "[p]rovid[e] an impression that their information will not be used or transferred for unanticipated purposes."[46]

With respect to individuals who registered with Celsius through a social media account, the company provided for itself in the privacy policy "access to basic information from your social network account, such as your full name, home address, email address, birthdate, profile picture, friends list, personal description, as well as any other information you made publicly available on such account or agreed to share with us." As the FTC report noted, "while consumers certainly expect ISPs to use information about the websites they wish to visit in providing the internet services itself, they would likely be surprised at the extent of data that is collected, retained, and combined for purposes unrelated to providing the service, particularly in ways that could cause them harm."[47] The Debtors advised the Ombudsman that while Celsius had the functionality to harvest social media data, they used social media to permit users to access their accounts. They collected and retained geolocation data pursuant to restrictions on financial transactions in the USA Patriot Act.

Insufficient information is provided to consumers regarding the myriad of ways that their data can be used, transferred, or monetized, often burying such disclosures in the fine print of the privacy policy. The privacy policy reserves broad rights concerning how the company will use and share consumer data, essentially permitting them to use the data for virtually any purpose.

---

[45] *Supra* note 39.

[46] FTC Privacy Practices Report, *supra* note 45.

[47] *Id.*, *supra* note 45.

Celsius can share personal data with broad categories of entities described very generally in the Terms of Use and the privacy policy.[48]

The Debtors have advised the Ombudsman that the actual practice of Celsius was not to share data other than for Bank Secrecy Act (BSA)/regulatory compliance, security, and e-mail marketing (for their own products, never third party marketing). Account holders were informed during registration why the company needed to collect Know Your Customer (KYC) information.

A close reading through the details of the lengthy Celsius privacy policy reveals policies that benefit the company and could potentially undermine the privacy of the account holders. This point becomes particularly clear when comparing the general provisions in the privacy policy itself with its different and consumer-friendly provisions required for California residents and members of EU countries and the United Kingdom under GDPR and the UK Data Protection Act 2018.

Celsius will only keep the personal data as long as it is needed for a business reason. However, the company has the ability to define (or leave undefined) in the privacy policy what constitutes a business reason, giving them virtually unfettered discretion. Following the policy, Celsius can delete personal information if the company chooses to do so, but is not required to

[48] Celsius Terms of Use, Section 22. Disclosure of Celsius Account Information. We may disclose information to third parties about you, your Celsius Account, or the transactions you make:

1. where it is necessary for the provision of our Services under these Terms;
2. in order to verify the existence and condition of your Celsius Account for a third party, such as a referral partner;
3. for the purpose of conducting our AML and KYC checks and compliance with applicable laws;
4. If you give us written authorization;
5. In order to comply with any request or order by any government agency or competent court; or
6. As described in our Privacy Policy (https://celsius.network/privacy-policy/)

develop and follow a data retention and deletion policy according to appropriate criteria that would protect the data or account holders.[49]

The Celsius' privacy policy includes a statement on "Corporate Transactions" that states the company *may share* consumer data, including personal information, "in the event of a corporate transaction (e.g., sale of a substantial part of our business, merger, consolidation or asset sale of an asset or transfer in the operation thereof)."[50]

This provision provides the option but does not mandate that any particular personal records be included in the sale. It provides discretion for the Court to decide what personal and financial data will be sold, and what privacy measures should be in place to protect the privacy interests of the consumers. The Court has authority to direct that certain personal and financial records not be included in the sale if the circumstances warrant such a limitation.

Mitigating the Risks of Phishing and Internet Crimes

On October 5, 2022, the names of 603,497 individual retail customers, along with their recent Celsius account transactions, were published in the Statement of Financial Affairs (SOFA) and Schedules of Assets and Liabilities, Schedule F-1 Non-Priority Unsecured Retail Customer Claims, [ECF No. 974, filed 10/5/22], beginning at page 92. The following information was published:

- Schedule F Line Number
- Creditor's Name
- Address (redacted for individual account holders)
- Earn Account Transactions

[49] Celsius Terms of Use, Section 19 B. Your Right to Close Your Celsius Account ("we reserve the right (but have no obligation) to delete all of your information and Celsius Account data stored on our servers").

[50] Corporate Transactions: "We may share information, including Personal Information, in the event of a corporate transaction (e.g., sale of a substantial part of our business, merger, consolidation or asset sale of an asset or transfer in the operation thereof) of the Company. In the event of the above, the acquiring company or transferee will assume the rights and obligations as described in this Privacy Policy."

- Custody Account Transactions
- Withhold Account
- Collateral on Loan Receivable

Almost immediately thereafter, according to blogs on the Internet, someone created a searchable database of the published names and financial transactions. This information could be used to try to determine the identity of particular individuals who may have suffered losses in the case.[51] The most publicized website where the data was published was celsiusnetworth.com. A screenshot of the Celsius Net Worth landing page from the date it was published is available.

Counsel for the Official Committee of Unsecured Creditors (UCC) consulted their forensic experts and advised the Ombudsman that some Reddit sub-threads have links to the raw data of schedules/statements of financial affairs (https://github.com/0xDareDevil/Celsius). This raw data is still published online and can be uploaded into Excel spreadsheets.

In addition, Debtors' counsel Kirkland & Ellis filed three reports with the Court advising that account holders have been subject to phishing attacks from someone impersonating K&E employees and representing that they were writing to verify the details of investor claims in this case. Clearly, these phishing e-mails and texts were sent to entice users to click on a link that could result in installation of malware on their computers and provide information that could be used for identity theft or fraud. [ECF No. 1527, filed 11/30/22; ECF No. 1681, filed 12/12/22; ECF 1904, filed 1/22/23]. Phishing attacks are now among the most common causes of data breaches and have had particularly devastating consequences for companies and individuals.[52]

[51] Wayback Machine - https://web.archive.org/web/20221009145221/https://celsiusnetworth.com/.

[52] Phishing is often used in conjunction with a spoofed e-mail. It is the act of sending an e-mail falsely claiming to be a legitimate business in an attempt to deceive the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specified website. The website, however, is not genuine and was set up only as an attempt to steal the user's information. FBI Scams and Safety: Internet Fraud, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud.

The Ombudsman recommended and the Debtors agreed to create a new tab on the Stretto Celsius website to post the K&E phishing notices [ECF No. 1527, filed 11/30/22; ECF No. 1681, filed 12/13/22; ECF 1904, filed 1/22/23], as well as to advise account holders of where to file complaints about harassment, doxing,[53] phishing, and other potential Internet crimes. The Stretto cite provides the following information:

> To report spoofing or phishing attempts, or to report that you've been a victim, file a complaint with the FBI's Internet Crime Complaint Center (IC3), the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC).

3. Privacy and Cybersecurity Risks are Heightened with Digital Assets -- Cyber Incidents Involving Financial Institutions and Cryptocurrency

In its work focused on cybersecurity risks to financial institutions, the Carnegie Endowment for International Peace found that "[c]ybersecurity risks to the financial system have grown in recent years, in part because the cyber threat landscape is worsening; in particular, state-sponsored cyberattacks targeting financial institutions are becoming more frequent, sophisticated, and destructive."[54] The Carnegie Endowment published a timeline that chronicles ~ 200 cyber incidents targeting financial institutions since 2007. The timeline can be filtered by country, region, year, attribution, incident type, and actor type.[55]

---

[53] Center for Internet Security, *Election Security Spotlight – Doxing*, https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-doxing. (Doxing is the malicious identification and online publication of information about an individual. It can include Personally Identified Information (PII) or other sensitive, private, or damaging content about the individual or the individual's family members. Malicious actors dox victims in an attempt to harm them via the public exposure of their information. Publicly available information can be used in aggregate with information from paid services or illicitly gathered information. The aggregation of information enables malicious actors to turn otherwise harmless content into a damaging collective. For example, separately, a person's last name, place of work, or home address is generally innocuous. However, when this information is combined it could constitute PII and be weaponized against a target, especially if coupled with account information, passwords, and financial records.)

[54] Carnegie Endowment for International Peace, *Timeline of Cyber Incidents Involving Financial Institutions*, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

[55] *Id.*

More than $2 billion in digital currency was stolen in hacks in 2021."[56] Further, over $1.9 billion was stolen in cross-chain hacks[57] in the first half of 2022, according to crypto analytic firm Chainalysis.[58] Investor protection was identified as a key concern at the 2021 Global Technology Summit, given the risks associated with cryptocurrency transactions.[59]

Cyber criminals have exploited vulnerabilities in the crypto infrastructure, as well as compromised individual accounts to steal cryptocurrency assets. The hacker attacks are both profit-driven, as well as motivated by a desire to disrupt crypto exchanges. As well, crypto exchanges have been used to facilitate illegal activities. Criminal charges have been brought against the Russian owner of a cryptocurrency exchange that is alleged to have facilitated a "darknet market" for ransomware proceeds, fraudulent ID documents, and money laundering.[60]

The principal policy objectives of Executive Order 14067 (2022) focus on the importance of protecting consumers and investors in the digital assets ecosystem: [61]

> Sec. 5. Measures to Protect Consumers, Investors, and Businesses.
>
> (a) The increased use of digital assets and digital asset exchanges and trading platforms may increase the risks of crimes such as fraud and theft, other statutory and regulatory violations, privacy and data breaches, unfair and abusive acts or practices, and other cyber incidents faced by consumers, investors, and businesses. The rise in use of digital assets, and differences across communities, may also present disparate financial risk to

---

[56] David Yaffe-Bellany, *The Crypto World Is on Edge After a String of Hacks*, THE NEW YORK TIMES (Sep. 28, 2022), https://www.nytimes.com/2022/09/28/technology/crypto-hacks-defi.html.

[57] Individuals must use a cross-chain bridge to move their assets from one blockchain to another. They combine multiple structures such as custodian, debt issuer, and an oracle, and thus are vulnerable because of the multiple attack avenues hackers can exploit.

[58] Maria Gracia Santillana Linares, *Over $2 Billion Stolen This Year In Blockchain Bridge Hacks Expose DeFi's Achilles Heel*, FORBES (Aug. 18, 2022), https://www.forbes.com/sites/mariagraciasantillanalinares/2022/08/18/over-2-billion-stolen-this-year-in-blockchain-bridge-hacks-expose-defis-achilles-heel/.

[59] Konark Bhandari, *Takeaways From the 2021 Global Technology Summit*, CARNEGIE INDIA (March 21, 2022), https://carnegieindia.org/2022/03/21/takeaways-from-2021-global-technology-summit-pub-86679.

[60] Press Release, U.S. Dept. of Justice, *Founder and Majority Owner of Cryptocurrency Exchanged Charged with Processing Over $700 Million of Illicit Funds* (Jan. 18, 2023), https://www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-charged-processing-over-700-million.

[61] EO 14067, *supra* note 41.

> less informed market participants or exacerbate inequities. It is critical to ensure that digital assets do not pose undue risks to consumers, investors, or businesses, and to put in place protections as a part of efforts to expand access to safe and affordable financial services.

4. FBI Warnings: Cyber Criminals are Exploiting Vulnerabilities in Crypto Platforms, Stealing Investors' Cryptocurrency

Data protection is a vital concern for the Celsius account holders. The FBI has issued an extraordinary number of warnings that demonstrate the need to focus on cybersecurity in this case, consider the data that may be put at risk, and limit the amount of data being sold. These FBI warning put companies on notice that their crypto infrastructures and individuals' accounts may be vulnerable to cyber attacks and they need to take immediate steps to protect their crypto assets and account holders' investments.

Over the past three years, the FBI has issued warnings to investors that cyber criminals are increasingly exploiting vulnerabilities in decentralized finance (DeFi) platforms to steal cryptocurrency, causing investors to lose large amounts of money. The FBI advised that "[c]yber criminals seek to take advantage of investors' increased interest in cryptocurrencies, as well as the complexity of cross-chain functionality and the open source nature of DeFi platforms."

(1) Criminals Exploiting Vulnerabilities in Smart Contracts

In August 2022 the FBI warned that criminals are targeting smart contracts governing DeFi platforms to steal investors' cryptocurrency. A smart contract is a self-executing contract with the terms of the agreement between the buyer and seller written directly into lines of code that exist across a distributed, decentralized blockchain network.[62]

(2) ATM Crypto Scams

[62] FBI *Cyber Criminals Increasingly Exploit Vulnerabilities in Decentralized Finance Platforms to Obtain Cryptocurrency, Causing Investors to Lose Money*, Alert No. I-082922-PSA (Aug. 29, 2022), https://www.ic3.gov/Media/Y2022/PSA220829.

On November 4, 2021 the FBI warned that scams involving cryptocurrency ATMs and QR codes are on the rise. Cybercriminals have started to abuse QR codes to receive fraudulent cryptocurrency payments from their victims. [63]

(3) Warning to Cryptocurrency Owners, Exchanges of Ongoing Attacks

On July 9, 2021 the FBI issued a Private Industry Notification (PIN) focused on the multiple methods criminals have used to "ransack crypto-wallets." [64] Attackers are using several tactics to steal and launder cryptocurrency, including technical support fraud, SIM swapping (a/k/a SIM hijacking), and taking control of their targets' cryptocurrency exchange accounts via identity theft or account takeovers.

(4) SIM Swapping to Steal from Digital Currency Accounts

The FBI San Francisco Division warned: "The FBI has seen an increase in the use of SIM swapping by criminals to steal digital currency using information found on social media. This includes personally identifying information or details about the victim's digital currency accounts."[65]

---

[63] *The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment*, Alert Number I-110421-PSA (Nov. 4, 2021), https://www.ic3.gov/Media/Y2021/PSA211104

[64] Sergiu Gatlan, *FBI warns cryptocurrency owners, exchanges of ongoing attacks*, BLEEPING COMPUTER (July 9, 2021), https://www.bleepingcomputer.com/news/security/fbi-warns-cryptocurrency-owners-exchanges-of-ongoing-attacks/. Between May 2020 and May 2021, the U.S. Secret Service observed and received reports from victims regarding cybercriminals stealing cryptocurrency after:

- gaining access to victims' crypto exchange accounts after bypassing two-factor authentication;
- impersonating payment platforms or cryptocurrency exchange support staff in phone calls initiated by victims of online tech support scams; and
- SIM swap attacks targeting the customers of multiple phone carriers.

[65] *FBI San Francisco Warns the Public of the Dangers of SIM Swapping: Criminals Are Targeting Victims with Cryptocurrency and Other Digital Currency Accounts* (March 6, 2019), https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/fbi-san-francisco-warns-the-public-of-the-dangers-of-sim-swapping.

Generally, the attackers follow this pattern:

- ***Identify the victim***: Identify a victim likely to own a large amount of digital currency, particularly cryptocurrency. Identify the victim's mobile telephone number and the mobile phone carrier.

Two Massachusetts men were sentenced on October 19, 2022 for an extensive scheme to take over victims' social media accounts and steal their cryptocurrency using techniques such as "SIM swapping," computer hacking, and other methods.[66] In their attacks, the defendants targeted individuals who likely owned significant amounts of crypto assets in Coinbase or Block.io wallets (like cryptocurrency executives) or potential victims who controlled high-value "Original Gangster" (OG) Instagram and Tumblr accounts.

5. Federal Indictment for Destructive Cyberattacks, Theft, and Extortion Related to Cryptocurrency

A federal indictment unsealed in February 2021 charged three North Korean computer programmers with participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, steal and extort more than $1.3 billion of money and cryptocurrency from financial institutions and companies, create and deploy multiple malicious cryptocurrency applications, and develop and fraudulently market a blockchain platform.[67]

- ***Swap the SIM card*:** Socially engineer a customer service representative from the mobile phone company in order to port the victim's phone number to a SIM card and phone in the control of the attackers.
- ***Password resets*:** Initiate password resets on the victim's email, cloud storage, and social media accounts (password resets usually accomplished by text messages to the victim's telephone number).
- ***Access accounts*:** Gain access to the victim's accounts and identify digital currency keys, wallets, and accounts that may be stored in them. Defeat any SMS-based or mobile application-based two-factor authentication on any accounts with control of the victim's phone number.
- ***Steal currency*:** Transfer the digital currency out of the victim's account into accounts controlled by the attackers.

[66] Press Release, U.S. Dept. of Justice, *Two Men Sentenced for Nationwide Scheme to Steal Social Media Accounts and Cryptocurrency* (Oct. 19, 2022), https://www.justice.gov/opa/pr/two-men-sentenced-nationwide-scheme-steal-social-media-accounts-and-cryptocurrency.

[67] Press Release, U.S. Dept. of Justice, *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe: Indictment Expands 2018 Case that Detailed Attack on Sony Pictures and Creation of WannaCry Ransomware by Adding Two New Defendants and Recent Global Schemes to Steal Money and Cryptocurrency from Banks and Businesses while Operating in North Korea, China* (Feb. 17, 2021), https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

In addition to these criminal charges, in 2018 the Treasury Department Office of Foreign Assets Control (OFAC) sanctioned one entity and one individual tied to the Government of North Korea's malign cyber activities. U.S.

6. Cyber Attacks on Digital Assets Infrastructure and Investor Crypto Accounts

Many digital asset platforms have vulnerabilities that have been exploited by hackers. The table at Appendix C of this CPO Report provides examples of the huge losses and disruption to investors and companies from the various types of attacks on cryptocurrency platforms and investor accounts.

V. Possible Alternatives to Mitigate Potential Privacy Losses or Costs to Consumers

A. "Qualified Buyer" Criteria – Developed in Prior Bankruptcy Cases

While asset sales are conducted to maximize the value of the estate and the return to creditors, the Bankruptcy Code also recognizes the importance of protecting the privacy of the personal data of individual account holders. Thus due diligence is essential to ensure that the proposed Purchaser(s)/ New Company officers and directors have demonstrated the capability of

---

Dept. Treasury, Treasury Targets North Korea for Multiple Cyber-Attacks (Sep. 6, 2018), https://home.treasury.gov/news/press-releases/sm473.

The indictment alleged a broad array of criminal cyber activities undertaken by the conspiracy, in the U.S. and abroad, for revenge or financial gain. The schemes alleged include these charges related to crypto-currency:

- ***Creation and Deployment of Malicious Cryptocurrency Applications***: Development of multiple malicious cryptocurrency applications from 2018 through 2020 – including Celas Trade Pro, WorldBit-Bot, iCryptoFx, Union Crypto Trader, Kupay Wallet, CoinGo Trade, Dorusio, CryptoNeuro Trader, and Ants2Whale – which would provide the North Korean hackers a backdoor into the victims' computers.
- ***Targeting of Cryptocurrency Companies and Theft*** of tens of millions of dollars' worth of cryptocurrency, including $75 million from a Slovenian cryptocurrency company in 2017; $24.9 million from an Indonesian cryptocurrency company in 2018; and $11.8 million from a financial services company in New York in 2020 in which the hackers used the malicious CryptoNeuro Trader application as a backdoor.
- ***Spear-Phishing Campaigns***: Multiple spear-phishing campaigns from 2016-20 that targeted employees of United States cleared defense contractors, energy companies, aerospace companies, technology companies, and the U.S. Departments of State and Defense.
- ***Marine Chain Token and Initial Coin Offering***: Development and marketing in 2017 and 2018 of the Marine Chain Token to enable investors to purchase fractional ownership interests in marine shipping vessels, supported by a blockchain, which would allow the DPRK to secretly obtain funds from investors, control interests in marine shipping vessels, and evade U.S. sanctions.

  See, *US exposes North Korea blockchain plot to evade ship sanctions: Hackers induced investors to fraudulently use cryptocurrency to own shares in North Korean cargo vessels* (Sep. 17, 2021), https://www.freightwaves.com/news/us-exposes-north-korea-blockchain-plot-to-evade-ship-sanctions.

protecting the privacy of the records of Celsius account holders and the intention to abide by an appropriate privacy policy.

To that end, over the years since the privacy requirements of the Bankruptcy Code were enacted in 2005, Bankruptcy Courts have applied certain criteria to establish that a Purchaser is "qualified" and would protect the privacy of the consumer data it purchased.[68] The FTC reiterated the applicability of these conditions in the Radio Shack bankruptcy case.[69]

The CPO recommends that the following "Qualified Buyer" criteria discussed above apply to the proposed Purchaser or whatever new entity is created to implement the "asset recovery plan."

- **The Purchaser/ New Company is in the same line of business as the Debtors.**

There is more to a finding of "qualified buyer" than merely the nature of the bidder's business—due diligence includes an understanding of a potential Purchaser's background. In this case, due diligence should be conducted to evaluate the plan sponsor and the proposed CEO and officers and directors of the new "recovery company," whether they have demonstrated expertise in the crypto business, and have experience handling large amounts of highly sensitive personal data and protecting is appropriately. Given the documented problems with some crypto companies, the proposed CEO, Officers and Directors should be scrutinized carefully, including conducting a criminal background check (audits, investigations, indictments and convictions).

---

[68] *In re* Toysmart.com, *supra* note 11. *In re* Choxi, 16-13131 (SCC) (SD NY) (Chapman, J.); *In re* Century 21 Department Stores, 20-12097 (SD NY) (Chapman, J.); *In re* KB US Holding 20-22962 (SHL) (SD NY) (Lane, J); *In re* MKJC Hyundai, 20-42283, (SD NY) (Mazer-Marino, J.); *In re* Loot Crate, 19-11791-BLS (D DE) (Shannon, J.); *In re* NovaSom, 19-11734 (BLS) (D DE) (Shannon, J.); *In re* Hobbico, 18-10055 (KG) (D DE) (Gross J.); *In re* Circuit City Stores, 3:08-bk-35653 (ED VA) (Huennekens, J.); *In re* Coach Am Group Holdings, No. 12-10010 (KG) (Gross J.) (Bankr. D. Del.); *In re* Linens N Things, 08-10832 (CSS) (D DE) (Sontchi, J.).

[69] FTC Requests Bankruptcy Court Take Steps to Protect RadioShack Consumers' Personal Information. Letter to Consumer Privacy Ombudsman Describes Possible Conditions on Sale of Data (May 18, 2015), *In re* RadioShack Corporation, No. 15-10197 (BLS) (Bankr. D. Del.) (Shannon, J.), *available* https://www.ftc.gov/news-events/news/press-releases/2015/05/ftc-requests-bankruptcy-court-take-steps-protect-radioshack-consumers-personal-information.

Assessing risks to consumers is critical because after the sale or transfer is approved, the Court has no authority to monitor the operations of the Purchase/ New Company.

Celsius has developed a due diligence "checklist" that may be useful to evaluate potential new owners of the recovery corporation to "understand the background of a party and to identify from open source records whether there are any indicators of fraud, mismanagement, or negative reputation." Celsius Third-Party Due Diligence Screen Cyber Security, Intelligence (Jan. 2022).

- **The Purchaser/ New Company agrees to use the personal consumer records for the same purpose(s) as they were used previously by Celsius.**

This point addresses the well-established privacy principle that personal data should only be used for the same purpose(s) for which it was collected.

- **The Purchaser/ New Company agrees to comply with an appropriate website privacy policy.**

As stated above, if a new "recovery company" is created, this would provide an excellent opportunity to develop a new privacy policy that reflects the legitimate business interests of the company and protects the privacy of account holders' data.

- **The Purchaser/ New Company agrees that prior to making any "material change" to the privacy policy or using or disclosing personal information in a different manner from that specified in the privacy policy, it will notify consumers/ account holders and afford them an opportunity to Opt-out of the changes to those policies or the new uses of their personal information.**
- **The Purchaser/ New Company agrees to employ appropriate information security controls (technical, operational and managerial) to protect electronic personal and**

financial customer information, including user wallets, and encryption keys.[70]

The FTC Safeguards Rule (16 C.F.R. § 314) requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. It reflects core data security principles that all covered companies need to implement.[71] Section 314.4 of the Safeguards Rule identifies nine elements that the company's information security program must include.

- **The Purchaser/ New Company agrees to abide by all applicable federal, state, and international laws, including privacy, data breach notification, data disposal, and cybersecurity laws and laws prohibiting unfair, deceptive or abusive practices "UDAP," "do-not-track," "do-not-call," and "no spam" laws.**
- Other issues to consider in conducting due diligence on the proposed Purchaser include;
    - Is the Buyer (owners/ leadership) located outside the United States?
    - Will the sale or transfer involve moving assets outside the country?
        - Does the CFIUS process apply?
        - Can the EU or a country block the sale or portions of it?
    - Do U.S. states have an interest in the sale or transfer?

[70] The measures Celsius has taken to protect the privacy and security of its assets and the personal and financial data of account holders is described in the Declaration of Shiran Kleiderman, Chief Security Officer of Celsius Network LLC, with Respect to the Debtors' Security. [ECF 812, filed 9/14/22]

[71] *FTC Safeguards Rule: What Your Business Needs to Know*, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know#Customer_information. The Safeguards Rule took effect in 2003; the FTC amended it in 2021 to make sure the Rule keeps pace with current technology.

B. Exclude Inactive Accounts from the Sale or Transfer

1. Develop Data Retention Plan

IRS and other rules require Celsius to retain certain personal and financial information for specified periods of time – often five-seven years. A data retention plan must specify what entity, after the sale, will maintain and protect the data that must be retained but is not included in the sale or transfer to a new entity.

2. Plan Appropriate Disposal/Deletion of Personal and Financial Data

Determinations must be made for how to delete and dispose of the data after the retention period has expired. How will the data be deleted in accordance with the requirements of applicable U.S. state laws. A similar analysis should be conducted for the data belonging to residents of countries around the globe under applicable country laws.

VI. The Sale or Transfer Must Not Violate Applicable Non-Bankruptcy Laws

Section 363(b)(1) of the Bankruptcy Code provides that the sale may not violate any applicable non-bankruptcy law. This section provides the Court with a broad overview of the existing laws and rules that pertain to privacy and cybersecurity generally, and to financial institutions in particular. A determination can be made after the Debtor files its plan for the sale or platform of Celsius' digital retail platform as to the applicability of these statutes and rules.

As discussed previously, Executive Order 14067 (2022) sets forth the following principal policy objectives of the U.S. with respect to digital assets.[72] The emphasis on protecting consumers, investors, and businesses is relevant to the Court's consideration of the Celsius sale or transfer of the retail platform assets:

> (a) We must protect consumers, investors, and businesses in the United States. The unique and varied features of digital assets can pose significant financial risks to

[72] EO 14067, *supra* note 41.

> consumers, investors, and businesses if appropriate protections are not in place. In the absence of sufficient oversight and standards, firms providing digital asset services may provide inadequate protections for sensitive financial data, custodial and other arrangements relating to customer assets and funds, or disclosures of risks associated with investment. Cybersecurity and market failures at major digital asset exchanges and trading platforms have resulted in billions of dollars in losses.

In most cases, the privacy issues in this case can be addressed and resolved using a practical approach that makes good business sense, as outlined in section V of this CPO Report.

A. U.S. Financial Regulatory Framework

> 2021 was a transformative year for digital assets, and the stage is set for regulators to build a framework to govern this massive new market. Thus far, the regulatory response is best described as ad-hoc, rhetorical or driven by enforcement in some instances. The challenge in such a new and disruptive area will likely take years to finalize. Adding to the challenge is the ambiguous nature of digital assets themselves and the lack of standardized definitions, thus creating questions of overlap and jurisdiction.[73]

A Report by the Congressional Research Service (CRS) provides an informative overview of the current U.S. financial regulatory framework.[74] The financial regulatory system has been described as fragmented, with multiple overlapping regulators and a dual state-federal regulatory system.[75] The system evolved piecemeal, punctuated by major changes in response to various historical financial crises.

---

[73] Susannah Hammond and Todd Ehret, *Cryptos on the rise 2022: A complex regulatory future emerges*, THOMSON REUTERS (2022), https://www.thomsonreuters.com/en/reports/cryptos-on-the-rise-2022.html.

> The compendium to this report provides a summary of the regulatory picture in each jurisdiction. It is grouped by region and focuses primarily on cryptocurrencies such as bitcoin. It provides an overview for each country, the regulatory state of play and links to the primary financial regulatory authorities or other relevant information.
>
> The United States is home to the largest number of crypto investors, exchanges, trading platforms, crypto mining firms and investment funds. The regulatory framework for cryptocurrencies is evolving despite overlap and differences in viewpoints between agencies. The SEC often views many cryptos as securities, the CFTC calls bitcoin a commodity, and Treasury calls it a currency.

[74] Congressional Research Service, *Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework Report* R44918*,* Summary (updated March 10, 2020), https://crsreports.congress.gov ["CRS Regulatory Framework Report."]

[75] At the federal level, regulators can be clustered in the following areas:

Before 1978, bank customers had no legal right to privacy with regard to financial information held by those institutions. However, the Right to Financial Privacy Act of 1978 (RFPA)[76] added some protections at the federal level. For decades now, individual financial records have been considered among the most sensitive and confidential personal records. Their privacy must be protected.

To address a prior financial crisis, Congress passed the Gramm-Leach-Bliley Act of 1999 (GLBA), P.L. 106-102, [77] and the Fair Credit Reporting Act (FCRA), P.L. 90-321.[78] In addition to reforming the financial services industry, GLBA addressed concerns relating to consumer financial privacy and enacted certain limitations on the disclosure of nonpublic personal information.

The most recent financial crisis resulted in changes to the regulatory system through the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010 (Dodd-Frank Act), P.L.

- Depository regulators—Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), and Federal Reserve for banks; and National Credit Union Administration (NCUA) for credit unions;
- Securities markets regulators—Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC);
- Government-sponsored enterprise (GSE) regulators—Federal Housing Finance Agency (FHFA), created by HERA, and Farm Credit Administration (FCA); and
- Consumer protection regulator—Consumer Financial Protection Bureau (CFPB), created by the Dodd-Frank Act. *Id.*

Other entities that play a role in financial regulation are interagency bodies, state regulators, and international regulatory fora. Notably, federal regulators generally play a secondary role in insurance markets. CRS Regulatory Framework Report, Summary, *supra* note 76.

[76] The 1978 Right to Financial Privacy Act (RFPA) established specific procedures that federal government authorities must follow in order to obtain information from a financial institution about a customer's financial records.

[77] Gramm-Leach-Bliley Act of 1999 (GLBA), P.L. 106-102, 15 U.S.C. § 6801; § 6801(b) Financial Institutions Safeguards.

[78] Fair Credit Reporting Act (FCRA), P.L. 90-321, 15 U.S.C. §§1681-1681x, Title VI of the Consumer Credit Protection (CCP) Act. *See*, https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act. The CCP Act protects information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services. Information in a consumer report cannot be provided to anyone who does not have a purpose specified in the Act.

111-203 and the Housing and Economic Recovery Act of 2008 (HERA), P.L. 110-289. To address the fragmented nature of the system, the Dodd-Frank Act created the Financial Stability Oversight Council (FSOC), a council of regulators and experts chaired by the Treasury Secretary.

The FTC has been the chief federal agency on privacy policy and enforcement since the 1970s. Since then, rapid changes in technology have raised new privacy challenges. The Dodd-Frank Act transferred primary responsibility for financial privacy to the Consumer Financial Protection Board (CFPB), but the FTC retains its enforcement authority.

The current regulatory treatment of crypto-assets depends on the facts and circumstances of the crypto-asset, the nature of the activities, and the classification of entities or service providers. Executive Order 14067 directed the CFPB and other regulators, including the FTC, to address consumer protection, data privacy, and competition issues in the crypto market.

Regulators can be categorized into the three main areas of finance—banking (depository), securities, and insurance (where state, rather than federal, regulators play a dominant role). There are also targeted regulators for specific financial activities (consumer protection) and markets (agricultural finance and housing finance).[79]

The existing regulatory system covers large parts of the crypto-asset ecosystem, with some gaps identified by the Financial Stability Oversight Council (FSOC). Its report concludes

[79] Regulators regulate financial institutions, markets, and products using licensing, registration, rulemaking, supervisory, enforcement, and resolution powers. In practice, regulatory jurisdiction is typically based on charter type, not function. In other words, how and by whom a firm is regulated depends more on the firm's legal status than the types of activities it is conducting. This means that a similar activity being conducted by two different types of firms can be regulated differently by different regulators. Financial firms may be subject to more than one regulator because they may engage in multiple financial activities. For example, a firm may be overseen by an institution regulator and by an activity regulator when it engages in a regulated activity and by a market regulator when it participates in a regulated market. Financial regulation aims to achieve diverse goals, which vary from regulator to regulator: market efficiency and integrity, consumer and investor protections, capital formation or access to credit, taxpayer protection, illicit activity prevention, and financial stability. CRS Regulatory Framework Report, *supra* note 76, Summary and page 7.

that "[c]ompliance with and enforcement of the existing regulatory structure is a key step in addressing financial stability risks."[80]

U.S. federal financial regulatory agencies with authority to address violations arising from the conduct risks associated with crypto-assets may include market regulators, banking regulators, agencies responsible for safeguarding the financial system from illicit use, and agencies with authority to enforce consumer protection laws. In addition, state agencies, including state securities and banking regulators often have authorities under state laws that apply to aspects of the crypto-asset ecosystem.[81]

B. Applicable Non-Bankruptcy Laws – Current U.S. Legal Landscape

No single federal law comprehensively regulates the collection and use of consumers' personal data. Some governments—such as California and the European Union (EU)—have recently enacted privacy laws regulating nearly all forms of personal data within their jurisdictional reach. In the U.S. federal privacy laws are sector-specific and many privacy protections are provided in state laws. In addition, the Debtors and the Purchaser must abide by the European Union and country laws when processing, transferring or disposing of the data of investors who reside in those jurisdictions.

1. Unfair, Deceptive, or Abusive Acts and Practices (UDAAP)

The FTC and CFPB have unique powers to protect consumers against "unfair" and "deceptive" acts and practices—with the CFPB also having additional powers to address "abusive" acts and practices. Those broad enforcement authorities encompass the key areas of fraud protection and consumer privacy with respect to digital assets. Unfair, deceptive, or

[80] Fact Sheet: *The Financial Stability Oversight Council's Report on Digital Asset Financial Stability Risks and Regulation*, October 3, 2022, https://home.treasury.gov/system/files/261/Fact-Sheet-Report-on-Digital-Asset-Financial-Stability-Risks-and-Regulation.pdf.

[81] CRS Regulatory Framework Report, *supra* note 76.

abusive acts and practices (UDAAP) can cause significant financial injury to consumers, erode consumer confidence, and undermine the financial marketplace.

The Consumer Financial Protection Bureau (CFPB) regulates the offering of consumer financial products and services – which, depending on the facts and circumstances, may include a variety of crypto-asset related offerings – under the federal consumer financial laws, including (among others) the Dodd-Frank Act's prohibition against unfair, deceptive, or abusive acts or practices for consumer financial products and services. The CFPB has supervisory authority for detecting and assessing risks to consumers and to markets for consumer financial products and services.

Recent interpretations of federal law provide examples of what may constitute an unfair, deceptive, or abusive act or practice. The *Joint Statement on Crypto-Asset Risks to Banking Organizations* provides the opinion of the three federal banking agencies that "[i]naccurate or misleading representations and disclosures by crypto-asset companies, including misrepresentations regarding federal deposit insurance, and other practices that may be unfair, deceptive, or abusive," are contributing to significant harm to retail and institutional investors, customers, and counterparties.[82]

Inadequate security for the sensitive consumer information collected, processed, maintained, or stored by the company can constitute an unfair practice in violation of 12 U.S.C. 5536(a)(1)(B). Guidance issued by the CFPB with respect to the adequacy of cybersecurity provides an instructive interpretation of UDAAP under the Dodd-Frank Act:[83]

---

[82] https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230103a1.pdf.

[83] CFPB, Consumer Financial Protection Circular 2022-04, https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.

> Acts or practices are unfair when they cause or are likely to cause substantial injury that is not reasonably avoidable or outweighed by countervailing benefits to consumers or competition. Inadequate authentication, password management, or software update policies or practices are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers, and financial institutions are unlikely to successfully justify weak data security practices based on countervailing benefits to consumers or competition. Inadequate data security can be an unfair practice in the absence of a breach or intrusion."

Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. Sec. 45(a)(1).[84] An act or practice is unfair if (1) it causes or is likely to cause substantial injury, (2) the injury is not reasonably avoidable by consumers, and (3) the injury is not outweighed by benefits to consumers or competition. 15 U.S.C. Sec. 45(n). "Deceptive" practices are defined in the Commission's Policy Statement on Deception[85] as involving a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances. The FTC has brought many cases alleging that the failure to adhere to promises about privacy constitute a deceptive practice under the FTC Act.

"Unfair business practices" is an evolving concept reflecting the ingenuity of unscrupulous business persons in concocting new schemes to gain advantage at someone else's expense. The FTC has identified several factors to be considered in determining whether a practice is unfair. The injury must be substantial, outweigh any countervailing benefit to the consumer, and be one the consumer cannot reasonably avoid.

---

[84] FTC *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority* (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority. FTC *Report to Congress on Privacy and Security* (Sep. 13, 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

[85] See FTC Policy Statement on Deception (Oct. 23, 1984) (appended to *Cliffdale Assocs., Inc.,* 103 F.T.C. 110, 183 (1984)), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

With respect to privacy, the FTC has adopted widely-accepted principles concerning fair information practices[86] and enforces laws prohibiting unfair and deceptive practices. This include cases against companies that make false or misleading statements in their privacy policies. Under Section 5, the FTC has pursued privacy and data security cases in myriad areas, including against social media companies, mobile app developers, data brokers, ad tech industry participants, retailers, and companies in the Internet of Things space.

2. Privacy of Consumer Financial Information

Federal law protects financial information, including credit card numbers, and provides certain requirements for providing notice of an organization's privacy policy and an opportunity for consumers to opt-out of changes to that policy.

Title V of the GLB Act set forth privacy requirements for the use of nonpublic personal financial information by banks, securities industry members, insurance companies, and other financial institutions.[87] The Financial Privacy Rule governs how financial institutions can collect and disclose customers' personal financial information; the Safeguards Rule requires all financial institutions to maintain safeguards to protect customer information; and another provision will prevent individuals and companies from gaining access to consumers' personal financial information under false pretenses, a practice known as "pretexting." The Act also limits the sharing of bank account number information for marketing purposes.

The CFPB issued Regulation P that requires financial institutions to develop and give notice of their privacy policies to their own customers at least annually and before disclosing any

[86] FTC Report—*Privacy Online: Fair Information Practices in the Electronic Marketplace*, www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[87] Privacy Rule, 16 C.F.R. Part 313 (May 24, 2000). FTC, *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act#exceptions.

consumer's personal financial information to an unaffiliated third party, and to give notice and an opportunity for that consumer to Opt-out from such disclosure. It also requires financial institutions and others to comply with limitations on redisclosure and reuse. 12 CFR Part 1016 (Sept. 17, 2018)

This statute and rules do not require consumers to receive notice and an opportunity to Opt-out of the disclosure of their personal data when an entire business is sold.[88] However they clearly do not preclude such notice and Opt-out process. Until the Debtors present their plan for the sale or transfer, no determination can be made concerning whether an Opt-out process would be required. However, in the future the Court may wish to consider, in a sound exercise of discretion, providing for an Opt-out in the circumstances of this case, *i.e.*, large amounts of sensitive data, a new cryptocurrency environment with widespread cybersecurity risks, and a privacy policy that is biased in favor of business interests. None of these factors were present when the Gramm-Leach-Bliley Act and other regulations were contemplated and issued.

The Celsius privacy policy shows how the company has already determined that such discretion can be exercised by creating a process for California residents to Opt-out of a sale:

> **Additional Information for California Residents**
> *Our Disclosure, Sharing of Personal Information*
>
> We do not sell your personal information.
>
> **California Resident's Rights Under the CCPA**

[88] 16 C.F.R. § 313.15 Other exceptions to notice and opt out requirements.

(a) Exceptions to opt out requirements. The requirements for initial notice in § 313.4(a)(2), for the opt out in §§ 313.7 and 313.10, and for service providers and joint marketing in § 313.13 do not apply when you disclose nonpublic personal information:

> (6) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit.

> If your personal information is subject to the CCPA, you may have certain rights with regard to such personal information, including the right to:
>
> Opt-Out of Sale. Request that we not sell your personal information if a business sells your personal information (we do not).

In light of the circumstances of this case and the sensitive nature of the personal data, the Court should consider requiring notice and an opportunity for all account holders to Opt-out of the sale.

3. Safeguards Rule – Cybersecurity Standards

Section 501 of the GLBA directed the FTC (and other agencies) to establish appropriate standards for financial institutions to keep customer information secure. The FTC issued the Safeguards Rule that requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. The policies and procedures must be reasonably designed to: (i) insure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (iii) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[89]

4. Red Flags Rule – Identify Theft Prevention

The Red Flags Rule,[90] requires many businesses and organizations to implement a written identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage.[91] The Rule tells

[89] *FTC Safeguards Rule: What Your Business Needs to Know* (2021), https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.

[90] Pub. L. 108-159 (2007) 16 C.F.R. § 681.1, *Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business*, https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business

[91] In 1988 Congress passed the Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028(a)(7). This legislation created a new offense of identity theft, which prohibits:

companies how to develop, implement, and administer an identity theft prevention program. A program must include four basic elements that create a framework to deal with the threat of identity theft. Identifying and detecting fraud includes spotting suspicious patterns to prevent the costly consequences of identity theft.

5. Children's Online Privacy Protection Act of 1998 (COPPA)

COPPA prohibits unfair or deceptive acts or practices in connection with the collection, use, or disclosure of PII from or about children under age 13 obtained on the Internet.[92] 16 CFR Part 312. Celsius states the following in its privacy policy concerning "minors":

> Minors
> The Services are not designated to individuals under the age of 18. If you are under 18 years old, you should not download the Application, use the Services, or provide any Personal Information to us. We reserve the right to access and verify any Personal Information collected from you. In the event that we become aware that an individual under the age of 18 has shared any information, we will delete such information within a reasonable time. If you have any reason to believe that an individual under the age of 18 has shared any information with us, please contact us at info@celsius.network.

For account holders who logged into Celsius through a social media account, it is possible that Celsius collected personal data about children in connection with the company's access to these social media accounts.

> [K]nowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

[92] FTC Children's Online Privacy Protection Rule ("COPPA"), 15 U.S.C. 6501-05. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

6. State Laws – Unfair and Deceptive Practices (UDP)

As with Section 5 of the FTC Act, states have enacted their own consumer protection laws that similarly prohibit unfair and deceptive acts or practices.[93] Many state laws also prohibit unfair or unconscionable practices, and a few prohibit abusive practices.

All 50 states have Unfair and Deceptive Acts and Practices (UDAP) laws that have been used to bring cases against companies that have false or misleading statements in their privacy policies posted online.

7. State Laws Related to Digital Privacy[94]

Because the U.S. does not have a comprehensive federal privacy law, several U.S. states have created their own privacy laws. These laws follow the FIPPs to afford specific protections to individuals and place clear obligations on businesses that collect and use personal data. Five states have enacted comprehensive consumer privacy laws:[95]

- California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 et seq.) and California Consumer Privacy Rights Act, 2020 (Proposition 24)
- Virginia Consumer Data Protection Act, 2021 H.B. 2307|2021 S.B. 1392 (Effective Jan. 1, 2023.)
- Colorado Privacy Act, 2021 S.B. 190 (Effective July 1, 2023.)
- Connecticut 2022 S.B. 6 (Personal Data Privacy and Online Monitoring) (Effective July 1, 2023.)

[93] Carolyn Carter, Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws (2018), NATIONAL CONSUMER LAW CENTER, https://www.nclc.org/resources/how-well-do-states-protect-consumers/. Appendix A – Capsule Summaries Of Strengths And Weaknesses Of Each State's UDAP Statute.

[94] National Conference of State Legislatures (NCSL), State Laws Related to Digital Privacy (updated June 7, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx; NCSL 2022 Consumer Privacy Legislation (June 10, 2022), https://www.ncsl.org/about-state-legislatures/2022-consumer-privacy-legislation.

International Association of Privacy Professionals (IAPP), US State Privacy Legislation Tracker 2022, Comprehensive Consumer Privacy Bills, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

[95] *See*, IAPP, *US State Privacy Legislation* Tracker (updated Oct. 7, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

- Utah Consumer Privacy Act, 2022 S.B. 227 (Effective Dec. 31, 2023.)

California Privacy Protection Act (CCPA)[96]

Celsius has nearly 50,000 account holders located in California. This broad-based technology-neutral privacy legislation governs access and deletion rights, and the notice and choices that companies must provide to California residents. The CCPA gives consumers more control over the personal information that businesses collect about them. This law secures privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information.

Businesses are required to give consumers certain notices explaining their privacy practices.

8. State Data Breach Notification Laws and Data Protection Provisions

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach notification laws that require any business in possession of certain sensitive personal information about a covered individual to disclose a security breach of that information to the person(s) affected.[97] State Attorneys General are enforcing a variety of the consumer protection, data breach notification laws and data disposal that are relevant in bankruptcy cases.

The largest number of Celsius account holders are located in the following U.S. states:

[96] State of California Department of Justice, Xavier Becerra, Attorney General, https://oag.ca.gov/privacy/ccpa

[97] NCSL Security Breach Notification Laws, *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

	State	Investor Count			State	Investor Count
	Total	233,228				
1	California	49,278		11	North Carolina	5,999
2	Florida	21,390		12	Massachusetts	5,986
3	Texas	18,367		13	Michigan	5,727
4	New Jersey	9,268		14	Ohio	5,691
5	Illinois	9,037		15	New York	4,097
6	Pennsylvania	8,400		16	Maryland	4,712
7	Georgia	7,346		17	Nevada	4,110
8	Virginia	6,370		18	Oregon	3,961
9	Colorado	6,365		19	Minnesota	3,916
10	Arizona	6,226		20	Tennessee	3,743

A number of states require companies that maintain certain personal information of state residents to take steps to protect against data breaches through data security measures, as well as secure disposal of personal information. At least 24 states have laws that address data security practices of private sector entities. Most of these data security laws require businesses to implement and maintain "reasonable security procedures and practices" appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.[98]

Below are examples of specific security requirements in the laws of states where large numbers of Celsius customers are located:

- ***California*** – Data custodians must implement reasonable security procedures and practices.
- ***Florida*** – Requires "reasonable measures to protect and secure data in electronic form containing personal information."[99]
- ***New York –*** Companies must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of private information including, but not limited to, disposal of data.[100]

[98] NCSL, Data Security Laws, Private Sector (May 29, 2019), *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[99] Florida Information Protection Act of 2014 (SB 1524) (Fla. Stat. § 501.171).

[100] New York Gen. Bus. Law s 899-BB; data breach notification N.Y. Gen. Bus. Law § 899-AA.

9. State Data Disposal Laws

At least 35 states and Puerto Rico have laws that govern the disposal of personal data held by businesses.[101] The laws, that require persons or entities to destroy, dispose of, or otherwise make personal information unreadable or undecipherable, will protect the privacy of the individuals who are Celsius customers. For example, Section 399-H of the New York General Business Law provides that a person or entity must dispose of materials containing personal information in a manner "consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record."[102]

C. Privacy Laws of the European Union[103] and Country Laws

More than 120 countries have privacy laws for data protection to ensure that citizens and their data are offered rigorous protections and controls.[104] Of the 600,000 Celsius active account holders, 366,772 individuals reside outside the U.S. in more than 200 countries around the world. Nearly 150,000 of these customers are located in the 27 EU countries.

1. European Union (EU) General Data Protection Regulation (GDPR)

The European Union (EU) GDPR[105] contains requirements related to consumer consent, mandatory data breach notification, and data management and portability. The law mandates that

---

[101] *See* NCLS, Data Disposal Laws, https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

[102] N.Y. Gen. Bus. Law § 399-H.

[103] The 27 EU countries are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

[104] IAPP Global Comprehensive Privacy Law Mapping Chart (April 2022), https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf; Online Consumer Protection Legislation Worldwide, United National Conference on Trade and Development (UNCTAD), https://unctad.org/page/online-consumer-protection-legislation-worldwide.

[105] *See* GDPR Portal, *available at* https://www.eugdpr.org/.

all businesses with European customers must fully adopt GDPR principles, including an adequate security strategy and technical measures to protect the personal data of EU citizens.

The six GDPR data protection principles are: (1) Lawfulness, fairness and transparency; (2) Purpose limitation; (3) Data minimization; (4) Accuracy; (5) Storage limitation; and (6) Integrity and confidentiality.

The GDPR has an extra-territorial effect. The Directive applies to all companies processing the personal data[106] of data subjects residing in the EU, regardless of the company's location. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU.

2. Country Privacy Laws

The laws and regulations that address personal data protection vary significantly from region to region or even country to country. The table below provides a list of the countries where the largest number of Celsius account holders reside, and the international privacy and data protection laws in each of those countries. More than 200 countries are represented among Celsius account holders.

	Country	EU	Count	Privacy Laws
			603,328	**Total Active Accounts**
1	United States		232,162	
2	Australia		27,576	Privacy Act of 1988, https://www.ag.gov.au/rights-and-protections/privacy
3	Canada		27,422	Personal Information Protection and Electronic Documents Act (PIPEDA), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

[106] Any information related to a natural person or 'data subject' that can be used to directly or indirectly identify the person, including a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

4	United Kingdom		24,220	UK Data Protection Act 2018 (UK-GDPR), https://www.gov.uk/data-protection
5	France	EU	21,072	GDPR
6	Italy	EU	20,369	GDPR
7	Argentina		17,360	Personal Data Protection Act 25.326 (PDPA)
8	Netherlands	EU	14,520	GDPR
9	Germany	EU	13,222	German Federal Data Protection Act
10	Singapore		13,321	Personal Data Protection Act (PDPA), https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act
11	Hong Kong		10,355	Personal Data (Privacy) Ordinance ("PDPO")[107]
12	Spain	EU	10,293	GDPR
13	India		8,279	Digital Personal Data Protection (proposed)
14	Poland	EU	7,914	GDPR
15	Malaysia		7,461	Personal Data Protection Act 2010 (PDPA)
16	Switzerland		7,034	Federal Act on Data Protection 1992 (FADP), https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en
17	Portugal	EU	6,633	GDPR
18	Belgium	EU	6,518	GDPR
19	Denmark	EU	5,926	GDPR as supplemented by the Danish Data Protection Act.
20	Czech Rep	EU	5,925	GDPR
21	Turkey		5,065	Law on The Protection Of Personal Data (DPL) No. 6698
22	Russian Fed		4,904	Federal Law No. 152-FZ (2006) as amended.
23	Philippines		4,674	Data Privacy Act of 2012 or Republic Act No. 10173
24	New Zealand		4,545	Privacy Act 2020
24	Brazil		4,355	General Data Protection Law
25	Serbia		4,281	Data Protection Law
26	South Africa		4,090	Protection of Personal Information Act (POPIA)
27	Ireland	EU	3,519	GDPR
28	Croatia	EU	3,334	GDPR
29	Thailand		3,196	Personal Data Protection Act (PDPA),
30	Sweden	EU	3,190	GDPR
31	Romania	EU	3,072	GDPR
32	Austria	EU	2,983	GDPR
33	Hungary	EU	2,952	GDPR
34	Slovakia	EU	2,767	GDPR
35	Greece	EU	2,740	GDPR
36	Columbia		2,391	Law 1266 and Law 1581
37	Slovenia	EU	2,308	GDPR
38	Sri Lanka		2,222	Personal Data Protection Act, No. 9 of 2022
39	Taiwan		2,108	Personal Data Protection Act
40	United Arab Emirates		2,076	Personal Data Protection Law, https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws
			Account holders also include the other 8 EU countries: Bulgaria 1,723, Cyprus 784, Estonia 680, Finland 1,796, Latvia 639, Lithuania 1,250, Luxembourg 578, Malta 554.	

[107] https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html.

VII. Conclusion

The issues related to the sale or transfer of the personal and financial records of the 1.7 million Celsius account holders required under the Bankruptcy Code have been addressed, including compliance with the privacy policy, the application of non-bankruptcy laws, and the losses or gains, and costs or benefits to consumers, if the sale or transfer is approved.

The Ombudsman has provided an analysis of the laws and privacy principles relevant to the proposed sale or transfer of Celsius account holder data to a new entity, and preliminary recommendations regarding practical steps the parties can take to protect their privacy. This CPO Report outlines the considerations the Court would need to take into account in making a decision to approve the sale or transfer of the retail platform assets to a Qualified Buyer.

The Debtors advised the Ombudsman that there is no present plan to sell the personal data of customers with inactive accounts. This decision, if unchanged, will result in protecting the privacy interests of 1.1 million Celsius account holders.

In prior bankruptcy cases, many cited in this CPO Report, the Debtors and the proposed Purchaser(s) have conferred with the Ombudsman and agreed to practical measures to ensure the privacy of consumers whose personal data is to be sold. The Ombudsman stands ready to answer any questions from the Court and the parties, confer with the parties to identify the protections that should apply to the personal data of the Celsius account holders, and develop plans for data retention and disposal of the data not included in the sale.

Respectfully submitted,

/s/ Lucy L. Thomson

Lucy L. Thomson
Consumer Privacy Ombudsman

APPENDIX A
Celsius Terms of Use

Declaration of Alex Mashinsky,
Chief Executive Officer of Celsius Network LLC,
Providing Terms of Use Dating Back to February 18, 2018

[ECF No. 393, filed 8/8/22]

Celsius Privacy Policy

https://celsius.network/privacy-policy

Date

Introduction

Celsius Network LLC (**"us"**, **"we"** or **"Company"**), 50 Harrison St, Suite 209F, Hoboken NJ 07030, respects the privacy of our users (each, **"you"** or **"User"**) and is committed to protecting the privacy of Users who access, download, install or register to our mobile or web application (the **"Application"**), our website or any other online services we provide (collectively: the **"Services"**). This Privacy Policy outlines our practices with respect to collecting, using and disclosing your information when you use the Services. We encourage you to read the Privacy Policy carefully and use it to make informed decisions. By using the Services, you agree to the terms of this Privacy Policy and your continued use of the Services constitutes your ongoing agreement to the Privacy Policy. The Privacy Policy is a part of the Terms of Service and is incorporated therein by reference.

This Privacy Policy contains information on our use of your personal information in accordance with relevant laws and regulations, including, where applicable, the EU General Data Protection Regulation (2016/679) (the **"EU GDPR"**), the EU GDPR such as it forms part of the laws of the United Kingdom (**"UK"**) by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (the **"UK GDPR"**), the UK Data Protection Act 2018 and the California Consumer Privacy Act of 2018 (**"CCPA"**). The rights discussed in certain sections of this Privacy Policy may be subject to exemptions or other limitations under applicable law.

For users who are located in the European Economic Area (**"EEA"**) and/or the UK and subject to the EU GDPR and/or the UK GDPR (together, the **"GDPR"**), please review this Privacy Policy and see the below Section, **"EU/UK Based Users and the GDPR"** for a description of your rights and other information related to the GDPR.

For users who are California residents and subject to the CCPA, please review this Privacy Policy and see the below Section, **"Additional Information for California Residents"** for a description of your rights with regard to your personal information (as defined by the CCPA), additional disclosures, and our notice at collection.

In this Privacy Policy you will read about, among other things:

What Type of Information We Collect

In general, we collect information, including Personal Information, when you communicate with us and when you use our Services. The information we request from you will be the minimum required to provide you with our services. When we use the term "**Personal Information**" we mean any information about an individual from which that person can be identified. Information that is anonymous, aggregated, or deidentified is generally not considered Personal Information.

There are instances where we invite or request individuals to provide us with their Personal Information through our Application, website or otherwise (e.g. by email), and we may also collect some information automatically. Through your use of our Services and your interactions with us, you may provide us with Personal Information including:

- **Identifiers and similar information** such as, name, address, date of birth, email address, social security number, driver's license number, passport number, online identifiers, or other similar identifiers;
- **Certain information protected under federal or state laws** such as a signature or bank account or other financial information;
- **Characteristics of protected classifications** under certain federal or state laws, including gender, national origin, or marital status;
- **Commercial information**, including records of products or services purchased, obtained, or considered, or other purchasing histories or tendencies;
- **Internet or other electronic network activity information**, including interactions with our website or use of certain online tools;
- **Geolocation data**, such as information about your location or the location of your device;
- **Audio, electronic, visual**, or similar information, which could be collected during audio or video calls (including video conferences and similar functions);
- **Biometric data**, such as images, which may constitute biometric data in certain jurisdictions. We may use such data for the purpose of identification for fraud and anti-money laundering checks;

- **Professional or employment-related information**, including occupation, compensation, employer, and title;
- **Inferences drawn from any of the information identified above** to create a profile reflecting your preferences or similar information; and

Sources of Personal Information

We collect Personal Information about you directly from you and/or your intermediaries through sources on our website, our Application, when you register or sign-in to the Services via your social network account, including when the following happens:

- **Signing up for an account**: When you sign-up and register for the Services, you will be asked to provide us certain details about yourself. You may register for the Services through your social network account or directly through the Application or our website (if applicable).
- **Registering through social network account**: When you register or sign-in to the Services via your social network account (e.g., Facebook, Twitter, etc.), we will have access to basic information from your social network account, such as your full name, home address, email address, birthdate, profile picture, friends list, personal description, as well as any other information you made publicly available on such account or agreed to share with us. At all times, we will abide by the terms, conditions and restrictions of the social network platform.
- **Registering through the Application or our website (if applicable)**: When you register for the Services through the Application or our website, we may collect from you the following information: full name, email address, home address, hometown, nationality, birthdate, phone number, as well as information required for our compliance with regulatory Know Your Customer requirements, such as passport or other identification number, and any other information you agreed to share with us.
- **Voluntarily provided information**: We may collect information which you provide us voluntarily. For instance, when you respond to communications from us, communicate with us via email or share additional information about yourself through your use of the Services. We may also collect the feedback, suggestions, complaints and reports which you send to us. Please note that we may also collect complaints about you from other Users, which may include your Personal Information.
- **Communication Recording**: We may record communications between you and any of our representatives and/or other participants, including recordings of audio, video and video conference calls, conversations or communications. We may collect this information for the purpose of resolving complaints, or for the purpose of improving the overall quality of the Services, for training and/or instructional purposes, record keeping or otherwise in order to comply with a legal or regulatory requirement to which we are subject.
- **Device information**: We may collect Personal Information from your device. Such information may include geolocation data, IP address, unique identifiers (e.g., MAC address and UUID) as well as other information which relates to your activity through the Services.

For the avoidance of doubt, if we combine Personal Information with non-personal information, the combined information will be treated as Personal Information as long as it remains combined.

In addition, we may collect Personal Information from different sources, such as: our affiliates, our service providers, or our affiliates' service providers; public websites or other publicly accessible directories and sources, including bankruptcy registers, tax authorities, governmental agencies and departments, and regulatory authorities; and/or from credit reporting agencies, sanctions screening databases, or from sources designed to detect and prevent fraud or financial crimes. The relevant source may be responsible for obtaining the relevant consents from you (where applicable) to ensure you are happy with the ways in which your Personal Information will be used.

How We Use the Information

We use and share Personal Information in the manners described in this Privacy Policy. In addition to the purposes listed above, the information we collect, which may include your Personal Information, is used for our business or commercial purposes such as:

- To set up your account and to provide the Services.
- To identify and authenticate your access to the Services.
- To authenticate your identity for the purpose of compliance with regulatory Know Your Customer requirements.
- To send you relevant push notifications, which are based on different activities offered by the Services.
- To communicate with you and to keep you informed of our latest updates and newsletters.
- To market our website, products, and the Services.
- To serve you personalized advertisements when you use the Services.
- To perform research or to conduct analytics in order to improve and customize the Services to your needs and interests.
- To support and troubleshoot the Services and to respond to your queries.
- To investigate and resolve disputes in connection with your use of the Services.
- To detect and prevent fraudulent and illegal activity or any other type of activity that may jeopardize or negatively affect the integrity of the Services; and
- To investigate violations and enforce our policies, and as required by law, regulation or other governmental authority, or to comply with a subpoena or similar legal process or respond to a government request.

With Whom We Share the Information and for What Purpose

We do not rent, sell, or share your Personal Information with third-parties except as described in this Privacy Policy. We may share Personal Information with the following recipients: (i) our subsidiaries; (ii) affiliated companies; (iii) subcontractors and other third-party service providers; (iv) business partners (such as GEM, Coinify, Simplex and Wyre); (v) auditors or advisers of our

business processes; and (vi) any potential purchasers or third party acquirer(s) of all or any portion of our business or assets, or investors in the company.

In addition to the purposes listed in this Privacy Policy, we may share Personal Information with our recipients for any of the following purposes: (i) storing or processing Personal Information on our behalf (e.g., cloud computing service providers); (ii) processing such information to assist us with our business operations; (iii) carrying out your instructions or giving effect to your preferences in relation to the Services we provide (including if you wish to use services which our business partners provide); (iv) performing research, technical diagnostics, personalization and analytics. We may also disclose Personal Information or any information we may have about you if we have a good faith belief that disclosure of such information is helpful or reasonably necessary to: (i) comply with any applicable law, regulation, legal process or governmental request; (ii) enforce our policies, including investigations of potential violations thereof; (iii) investigate, detect, prevent, or take action regarding illegal activities or other wrongdoing, suspected fraud or security issues; (iv) to establish or exercise our rights to defend against legal claims; (v) prevent harm to the rights, property or safety of us, our affiliates, our Users, yourself or any third-party; (vi) for the purpose of collaborating with law enforcement agencies; and (vii) in case we find it necessary in order to enforce intellectual property or other legal rights.

Wherever possible, we will only disclose Personal Information to a third party in circumstances where that third party has agreed to respect the security and confidentiality of Personal Information and treat it in accordance with applicable law. We will seek to ensure that third parties to whom any Personal Information may be disclosed will not use Personal Information for their own purposes and only process Personal Information for specified purposes and otherwise in accordance with our instructions and/or with applicable laws.

We may also disclose Personal Information about you to a third party at your request or direction or with your consent.

Corporate Transactions

We may share information, including Personal Information, in the event of a corporate transaction (e.g., sale of a substantial part of our business, merger, consolidation or asset sale of an asset or transfer in the operation thereof) of the Company. In the event of the above, the acquiring company or transferee will assume the rights and obligations as described in this Privacy Policy.

Third-Party Collection of Information

Our policy only addresses the use and disclosure of information we obtain about you. To the extent that you disclose your information to other parties via the Services (e.g., by clicking on a link to any other website or location) or via other sites throughout the Internet, different rules may apply to their use or disclosure of the information you disclose to them. You acknowledge that we are not responsible for the products, services, or descriptions of products or services that you receive from third-party sites or to the content or privacy practices of those sites, and that this Privacy Policy does not apply to any such third-party products and services. You are

knowingly and voluntarily assuming all risks of using third-party sites to purchase products and services. You agree that we shall have no liability whatsoever with respect to such third-party sites and your usage of them.

Cookies and Google Analytics

We may use cookies and other technologies or methods of web and mobile analysis to gather, store, and track certain information related with your access to and activity through the Services, including when you visit our website.

Below, we describe the types of cookies (as defined below) we use, and how you can control our use of cookies.

Types of Cookies We Use

As mentioned above, we will collect certain information about you when you visit our website. We collect such information through the following technologies (collectively, "cookies"):

- Cookies. Cookies are small pieces of information that a website assigns to your device while you are viewing a website. Cookies may be served by the entity that operates the website you are visiting ("first-party cookies") or by other companies ("third-party cookies"). Additionally, some cookies may be temporary and erase when you close your browser ("session cookies"), and others may remain for a set duration ("persistent cookies").
- Log Files. Tools that track actions occurring on the site, and collect data including your IP address, browser type, Internet service provider, referring/exit pages, and date/time stamps.
- Web Beacons. These "tags" and "pixels" are electronic files used to record information about how you browse our website.
- Social Media Widgets. These are tools that allow us to provide certain social media features such as links to Facebook, Instagram, and Twitter. These social features are either hosted by a third party or hosted directly on our website. Your interactions with these features are governed by the privacy policy of the company providing it.

Cookies are very helpful and may be used for various different purposes such as delivering personalised services. These purposes include, among other things, allowing you to navigate between pages efficiently, enabling automatic activation of certain features, remembering your preferences and making the interaction between you and the Services quicker, easier and smoother. Our website may use the following types of cookies:

- **Strictly Necessary Cookies**. These cookies are required for the operation of our website, and are essential to enable you to login, navigate around and use the features of a website, or to provide a service requested by you. We do not need to obtain your consent in order to use these cookies.
- **Functionality Cookies**. These cookies allow the website to remember choices you make (such as your user name, language, or the region you are in) and provide enhanced, more

personal features. For instance, a website may be able to provide you with local weather reports or traffic news by using a cookie to store information about the region in which you are currently located, remember changes you have made to text size, fonts, and other parts of web pages that you can customize, and provide services you have asked for such as watching a video or commenting on a blog. The information these cookies collect remains anonymous and they cannot track your browsing activity on other websites.

- **Performance/Analytics Cookies**. These cookies allow us to recognize and count the number of visitors and to see how visitors use a website, for example which pages you go to most often, and record difficulties you may experience while using the Website, for example error messages. All information collected by these cookies is aggregated and therefore anonymous. It is only used to improve the efficiency of the website. We also use a tool called Google Analytics to collect information about your use of the Services. Google Analytics collects information such as how often users access the Services, what pages they visit when they do so, etc. We use the information we get from Google Analytics only to improve our Services. Google Analytics collects the IP address assigned to you on the date you visit sites, rather than your name or other identifying information. We do not combine the information collected through the use of Google Analytics with Personal Information. Google's ability to use and share information collected by Google Analytics about your visits to our website is restricted by theGoogle Analytics Terms of Service and the Google Privacy Policy.
- **Targeting/Advertising Cookies**. These cookies are used to deliver advertisements tailored to you and your interests. They are also used to limit the number of times you see an advertisement as well as help measure the effectiveness of the advertising campaign. They are usually placed by advertising networks with the website operator's permission. They remember that you have visited a website and this information is shared with other organizations such as advertisers. Quite often targeting or advertising cookies will be linked to site functionality provided by the other organization. For more information about online behavioral advertising cookies and online privacy, please see the guide produced by the internet advertising industry available at youronlinechoices.com.

How to Control Cookies

Your browser is likely set to accept cookies. However, if you would prefer not to receive them, you can alter the configuration of your browser to refuse cookies. If you choose to have your browser refuse cookies (as explained below), it is possible that some areas of our website will not function properly when you view them.

You can control our uses of cookies through your internet browser or through third party tools:

- **Internet Browser.** You can control cookies through most browsers by changing your cookie settings. These settings will typically be found in the "options" or "preferences" menu of your browser.
- **Third Party Tools.** You can also visit http://www.allaboutcookies.org/ where you will find comprehensive information on cookie management and blocking which pertains to a wide variety of cookies. As noted above, our website uses Google Analytics to collect information about how visitors are using our website. Google Analytics has its own

cookies that it uses to track and aggregate this information. You can prevent the use of Google Analytics relating to your use of our website by downloading and installing the browser plugin available here.

Advertisements and Advertising Tools

Advertisements

We may use a third-party advertising technology to serve advertisements when you use the Services. This technology uses your information with regards to your use of the Services to serve advertisements to you (e.g., by placing third-party cookies on your web browser). We may also use our third-parties and share with them Users' information to assist us in evaluating the success of our advertising campaigns and help us retargeting our Users.

Advertising ID and Advertising Identifier

The Google Advertising ID is an anonymous identifier, provided by Google Play services. If your device has an Advertising ID, we may collect and use it for advertising and user analytics purposes. We may also use Apple's Advertising Identifier (IDFA), which is a non-permanent device identifier provided by Apple, and any information obtained through the use of the Advertising Identifier, for the purpose of advertising. By downloading or using the Application or the Services you explicitly agree that we may associate your Advertising ID and your Advertising Identifier with your applicable persistent device identifier. This will facilitate our ability to improve your personalized experience. Further, we may use other persistent identifiers for non-advertising purposes. If your device does not have Advertising ID or Advertising Identifier respectively, we will use other identifiers.

How to Control Certain Advertising Technology

You may opt-out of many third-party ad networks, including those operated by members of the Network Advertising Initiative ("NAI") and the Digital Advertising Alliance ("DAA"). For more information about this practice by NAI and DAA members, and your choices regarding having this information used by these companies, including how to opt-out of third-party ad networks operated by NAI and DAA members, please visit their respective websites: https://optout.networkadvertising.org or https://optout.aboutads.info [EU users may opt out of receiving targeted advertising through the European Interactive Digital Advertising Alliance] You may also control your advertising preferences or opt-out of certain Google advertising products by visiting the Google Ads Preferences Manager, currently available at https://google.com/ads/preferences.

Additionally, your mobile device operating system may provide mechanisms that allow users to opt out of the use of information about their usage of mobile apps to deliver targeted ads to their mobile device. For more information, or to opt out using these mechanisms, consult your device settings.

For How Long We Retain Your Information

How long we keep your Personal Information will vary depending on the type of Personal Information and our reasons for collecting it. The retention period will be determined by various criteria, including the purposes for which we are using it (as it will need to be kept for as long as is necessary for any of those purposes) and our legal obligations (as laws or regulations may set a minimum period for which we have to keep your Personal Information). In general, we will retain your Personal Information for as long as we require it to perform our contractual rights and obligations, resolve disputes and enforce our policies and agreements, or for periods required by our legal and regulatory obligations.

How We Protect Your Information

We take great care in implementing and maintaining the security of the Services and your information. We will take reasonable steps and use technical, administrative and physical security measures appropriate to the nature of the information and that comply with applicable laws to protect Personal Information against unauthorized access and exfiltration, acquisition, theft, or disclosure. Although we take enhanced steps to safeguard information, given the nature of information security, there is no guarantee that such measures will always be successful. We cannot be responsible for the acts of those who gain unauthorized access or abuse the Services, and we make no warranty, express, implied or otherwise, that such access will be prevented. If you feel that your privacy was treated not in accordance with our policy, or if any person attempted to abuse the Services or acted in an inappropriate manner, please contact us directly at info@celsius.network.

Minors

The Services are not designated to individuals under the age of 18. If you are under 18 years old, you should not download the Application, use the Services, or provide any Personal Information to us. We reserve the right to access and verify any Personal Information collected from you. In the event that we become aware that an individual under the age of 18 has shared any information, we will delete such information within a reasonable time. If you have any reason to believe that an individual under the age of 18 has shared any information with us, please contact us at info@celsius.network.

EU/UK Based Users and the GDPR

If you are an EU or UK data subject and the processing of your Personal Information is subject to the GDPR, please review this section in addition to the entire Policy.

(I) Grounds for Processing

We will only process your Personal Information in circumstances where we have established a lawful basis to do so. Our lawful bases for processing that Personal Information include:

- *Legitimate Interests.* We process Personal Information for our legitimate business interest in managing and promoting our business, provided that our interest is not overridden by your interest. In identifying and relying on this basis for certain processing, we have

weighed our legitimate interest as a business against your rights and freedoms and have determined that such processing will not unfairly impact your rights. If you would like further information on how we balanced these interests, you can contact us using the details below. Please note that you have a right to object to the processing of your Personal Information where that processing is carried on for our legitimate interest.

- *Legal Requirements.* We may need to process your Personal Information in order to comply with certain legal and regulatory requirements, including to establish, exercise or defend legal claims, respond to a judicial process, law enforcement or governmental agency.
- *Contract.* Depending on the circumstances, we may need to process your Personal Information for the performance of a contract to which you are a party, or related pre-contractual steps.
- *Consent.* We may process your Personal Information with your consent, as required by the GDPR. You have the right to withdraw this consent at any time where we are relying on consent to process your Personal Information. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent.

(II) Your Rights under the GDPR

We respect your privacy rights and therefore you may contact us at any time and request:

• *Access.* You have the right to know we collect certain Personal Information about you and to ask us for copies of your Personal Information. Please use the contact details provided at the end of this Policy.

• *Rectification.* You have the right to request that we correct your Personal Information you think is inaccurate or incomplete.

• *Objection to processing.* You have the right to object to processing in some circumstances, including where we are using your Personal Information for our legitimate interests and for direct marketing purposes, including by opting-out of marketing communications by contacting us using the contact details provided at the end of this Policy.

• *Erasure.* You have the right to request that we erase the Personal Information we have collected about you in certain circumstances. The right to erasure is not absolute, and only applies if we no longer need your Personal Information to carry out the purpose that we collected it for, whilst in compliance with laws applicable to us; you have withdrawn your consent to our use of your Personal Information; you have objected to our use of your Personal Information and your interests outweigh our interests in using it; you believe we have processed your Personal Information unlawfully; or we have a legal obligation to erase your data. Subject to our retention policies, we will consider any request to erase Personal Information for any of the above reasons and endeavour to comply with the request to the extent permitted by law, but we may not always be able to comply with your request. We may be required to retain the Personal Information for certain retention periods in order to comply with legal and regulatory requirements under applicable laws and regulations to which we are subject. If we are unable to comply with your

request, we will contact you in writing. If you wish to exercise this right, please contact us at: app@celsius.network.

• *Restrict processing.* You have the right to ask us to restrict the processing of your Personal Information in certain circumstances, including if you have concerns regarding the accuracy of your Personal Information, where you have made an objection to our use of your personal data; or if you believe we processed your Personal Information unlawfully, but you do not want us to delete it.

• *Data portability.* You have the right to receive a copy of the Personal Information that we collect about you in a way that is accessible and in a machine-readable format where the processing is based on your consent, the performance of a contract with you, or carried out by automated means. You have the right to request that such Personal Information be transmitted directly from us to another data controller, where technically feasible.

• *Withdrawal of consent.* You can withdraw your consent at any time where we are relying on consent to process your Personal Information. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent.

However, please note that these rights are not absolute, and may be subject to our own legitimate interests and regulatory requirements.

We will store your Personal Information only for as long as necessary for the purposes for which it was collected, including to provide the Services and to comply with our legal obligations, resolve disputes and enforce our policies and agreements. Retention periods will be determined taking into account the type of information that is collected and the purpose for which it is collected, bearing in mind the requirements applicable to the situation and the need to destroy outdated, unused information at the earliest reasonable time. Under applicable regulations, we will keep records containing client Personal Information, account opening documents, communications and anything else as required by applicable laws and regulations.

We may rectify, replenish or remove incomplete or inaccurate information, at any time and at our own discretion. If you wish to make a complaint regarding our handling of your Personal Information, you can contact us at info@celsius.network. You may also make a complaint to the relevant supervisory authority for data protection issues. In the UK this is the Information Commissioner's Office ("**ICO**"). Contact details for the ICO may be found at www.ico.org.uk.

(III) Transfer of Information Outside the UK and/or the EEA

Please note that some data recipients may be located outside the EEA and/or the UK. In such cases we will seek to ensure a similar degree of protection is afforded to it by ensuring that, where possible, Personal Information is generally transferred only to persons in countries outside the EU or the UK in one of the following circumstances:

- transfers only to such countries as approved by the European Commission or the equivalent entity in the UK as providing adequate level of data protection;

- to persons and undertakings to whom the transfer of such Personal Information is made pursuant to a contract that is compliant with the model contracts for the transfer of Personal Information to third countries from time to time approved by the European Commission (as supplemented where and if required) or the equivalent body in the UK;
- to persons and undertakings outside of the EU or the UK pursuant to other appropriate safeguards for the transfer of Personal Information; and
- only on one of the conditions allowed under the GDPR in the absence of (i) a decision by the European Commission or the equivalent entity in the UK that has deemed a country to provide an adequate level of protection for Personal Information (i.e. an adequacy decision) or (ii) appropriate safeguards such as a contract that is compliant with the model contracts for the transfer of Personal Information to third countries approved by the European Commission or the equivalent entity in the UK.

You can contact us through the information provided below for further information on specific mechanisms we utilise for transferring Personal Information outside the EU or the UK and the countries to which such transfer may be made.

Additional Information for California Residents

The CCPA imposes certain obligations on us and grants certain rights to California residents ("California Resident," "you" or "your") with regard to "personal information" as defined by the CCPA. If you are a California Resident, please review the following information about our privacy practices surrounding how and why we collect, use, disclose, and share your personal information and your potential rights with regard to your personal information under the CCPA. The rights described in this section are subject to exemptions and other limitations under applicable law.

Terms used in this section have the meaning ascribed to them in the CCPA. We are a "business." "Personal information" as used in this section has the same meaning as in the CCPA. It does not include deidentified information, aggregate consumer information or publicly available information, as those terms are defined in the CCPA.

Notice at Collection and Use of Personal Information

What Type of Information We Collect

Depending on how you interact with us, we may collect the categories of personal information listed above in the section **"What Type of Information We Collect"** above.

How We Use Collected Information

We may use your personal information for the business or commercial purpose listed above in the section **"How We Use The Information"** and **"With Whom We Share The Information and For What Purpose"** above.

Our Collection, Use, Disclosure, and Sharing of Personal Information

What Information We Have Collected and the Sources from Which We Collected It

In the preceding 12 months, and depending on how you interact with us, we may have collected all or some of the personal information listed above in "**What Type of Information We Collect**" above. We may have collected personal information from all or some of the categories of sources listed in the above section, "**Sources of Personal Information**"

Purposes for Collecting Personal Information

We may collect the personal information for one or more of the following business or commercial purposes described in the above section, "**How We Use The Information**" and "**With Whom We Share The Information and For What Purpose**" above.

Our Disclosure, Sharing of Personal Information

We do not sell your personal information. We do not knowingly sell the personal information of California residents under 16 years old. We may disclose your personal information to certain third parties for a business purpose. In the preceding 12 months, we may have disclosed for a business purpose the following categories of personal information to the following categories of third parties:

Category of Personal Information	Category of Third Party Information Disclosed to for a Business Purpose
Identifiers and Similar Information (such as name, email or IP address)	• Entities who assist with fraud prevention, detection and mitigation, including credit agencies and to assist with anti-money laundering or anti-terrorism checks • Judicial courts, regulators, or other government agents purporting to have jurisdiction over the group or opposing counsel and parties to litigation • Providers or partners that support our business operations (such as banking partners; wallet providers; etc) • Affiliates • Marketing partners • Providers or partners that support our business operations (such as payment services providers, etc.)
Additional Information Protected by Certain Federal or State Laws (for example, financial information)	• Entities who assist with fraud prevention, detection and mitigation, including credit agencies and to assist with anti-money laundering or anti-terrorism checks • Judicial courts, regulators, or other government agents purporting to have jurisdiction over the

Category of Personal Information	Category of Third Party Information Disclosed to for a Business Purpose
	group or opposing counsel and parties to litigation
Characteristics Information (such as age or gender)	• Entities who assist with fraud prevention, detection and mitigation, including credit agencies and to assist with anti-money laundering or anti-terrorism checks • Judicial courts, regulators, or other government agents purporting to have jurisdiction over the group or opposing counsel and parties to litigation
Commercial Information (for example, products purchased)	• Affiliates • Entities who assist with fraud prevention, detection and mitigation, including credit agencies and to assist with anti-money laundering or anti-terrorism checks • Judicial courts, regulators, or other government agents purporting to have jurisdiction over the group or opposing counsel and parties to litigation
Internet and Electronic Network Activity Information (such as browsing history and your interactions with our website)	• Analytics providers
Geolocation Information (such as device location)	• Entities who assist with fraud prevention, detection and mitigation, including credit agencies and to assist with anti-money laundering or anti-terrorism checks • Judicial courts, regulators, or other government agents purporting to have jurisdiction over the group or opposing counsel and parties to litigation

APPENDIX B

Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency

January 3, 2023

Joint Statement on Crypto-Asset Risks to Banking Organizations

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing the following statement on crypto-asset[108] risks to banking organizations.

The events of the past year have been marked by significant volatility and the exposure of vulnerabilities in the crypto-asset sector. These events highlight a number of key risks associated with crypto-assets and crypto-asset sector participants that banking organizations should be aware of, including:

- Risk of fraud and scams among crypto-asset sector participants.
- Legal uncertainties related to custody practices, redemptions, and ownership rights, some of which are currently the subject of legal processes and proceedings.
- Inaccurate or misleading representations and disclosures by crypto-asset companies, including misrepresentations regarding federal deposit insurance, and other practices that may be unfair, deceptive, or abusive, contributing to significant harm to retail and institutional investors, customers, and counterparties.
- Significant volatility in crypto-asset markets, the effects of which include potential impacts on deposit flows associated with crypto-asset companies.
- Susceptibility of stablecoins to run risk, creating potential deposit outflows for banking organizations that hold stablecoin reserves.
- Contagion risk within the crypto-asset sector resulting from interconnections among certain crypto-asset participants, including through opaque lending, investing, funding, service, and operational arrangements. These interconnections may also present concentration risks for banking organizations with exposures to the crypto-asset sector.
- Risk management and governance practices in the crypto-asset sector exhibiting a lack of maturity and robustness.
- Heightened risks associated with open, public, and/or decentralized networks, or similar systems, including, but not limited to, the lack of governance mechanisms establishing oversight of the system; the absence of contracts or standards to clearly establish roles, responsibilities, and liabilities; and vulnerabilities related to cyber-attacks, outages, lost or trapped assets, and illicit finance.

[108] By "crypto-asset," the agencies refer generally to any digital asset implemented using cryptographic techniques.

It is important that risks related to the crypto-asset sector that cannot be mitigated or controlled do not migrate to the banking system. The agencies are supervising banking organizations that may be exposed to risks stemming from the crypto-asset sector and carefully reviewing any proposals from banking organizations to engage in activities that involve crypto-assets. Through the agencies' case-by-case approaches to date, the agencies continue to build knowledge, expertise, and understanding of the risks crypto-assets may pose to banking organizations, their customers, and the broader U.S. financial system. Given the significant risks highlighted by recent failures of several large crypto-asset companies, the agencies continue to take a careful and cautious approach related to current or proposed crypto-asset-related activities and exposures at each banking organization.

Banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation. The agencies are continuing to assess whether or how current and proposed crypto-asset-related activities by banking organizations can be conducted in a manner that adequately addresses safety and soundness, consumer protection, legal permissibility, and compliance with applicable laws and regulations, including anti-money laundering and illicit finance statutes and rules. Based on the agencies' current understanding and experience to date, the agencies believe that issuing or holding as principal crypto-assets that are issued, stored, or transferred on an open, public, and/or decentralized network, or similar system is highly likely to be inconsistent with safe and sound banking practices. Further, the agencies have significant safety and soundness concerns with business models that are concentrated in crypto-asset-related activities or have concentrated exposures to the crypto-asset sector.

The agencies will continue to closely monitor crypto-asset-related exposures of banking organizations. As warranted, the agencies will issue additional statements related to engagement by banking organizations in crypto-asset-related activities. The agencies also will continue to engage and collaborate with other relevant authorities, as appropriate, on issues arising from activities involving crypto-assets.

Each agency has developed processes[109] whereby banking organizations engage in robust supervisory discussions regarding proposed and existing crypto-asset-related activities.[110] Banking organizations should ensure that crypto-asset-related activities can be performed in a safe and sound manner, are legally permissible, and comply with applicable laws and regulations, including those designed to protect consumers (such as fair lending laws and

---

[109] See OCC Interpretive Letter 1179 "Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank," (November 18, 2021); Federal Reserve SR 22-6 / CA 22-6: "Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations," (August 16, 2022); and FDIC FIL-16-2022 "Notification and Supervisory Feedback Procedures for FDIC-Supervised Institutions Engaging in Crypto-Related Activities," (April 7, 2022).

[110] Entities seeking to become regulated banking organizations will also be expected to adopt and demonstrate appropriate risk management processes and controls to mitigate risks associated with planned activities, which would include any crypto-asset-related activities, before receiving a charter or otherwise being authorized to commence business. The entities should discuss all planned activities with the appropriate regulator prior to filing an application.

prohibitions against unfair, deceptive, or abusive acts or practices). Banking organizations should ensure appropriate risk management, including board oversight, policies, procedures, risk assessments, controls, gates and guardrails, and monitoring, to effectively identify and manage risks.[111]

[111] See Interagency Guidelines Establishing Standards for Safety and Soundness 12 CFR 30, Appendix A (OCC); 12 CFR 208, Appendix D-1 (Federal Reserve) and 12 CFR 364, Appendix A (FDIC). See also OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, 12 CFR 30, Appendix D (OCC).

APPENDIX C

Cyber Attacks on Digital Assets Infrastructure and Investor Crypto Accounts

Vulnerabilities in many digital asset platforms have been exploited by hackers. The table below provides examples of the huge losses and disruption to investors and companies from the various types of attacks on cryptocurrency platforms and accounts.

When a trading platform is compromised by cybercriminals, its users face the risk of losing their funds due to theft. In addition to funds, an attacker can also steal application programming interface (API) keys from the trading platform. These keys can be used to program bots to withdraw funds from the account or to perform fraudulent trades.[112]

Date	**Company**	**Cyber Attack**	**Losses**
Attacks on Digital Infrastructure			
2014	Mt. Gox At the time the company handled 70% of all bitcoin transactions worldwide	Numerous problems ranging from mismanagement to security violations such as unencrypted passwords esulted in bankruptcy later that year.[113]	Hackers stole 740,000 bitcoin from customers and 100,000 from the company, equivalent of ~ $460 million (2014).
2018	Coincheck Suffered what appeared to be at the time the largest hack in the history of the technology.	In 2021 30 individuals were formally charged in Japan with trading almost $100 million worth of digital assets, including $560 million stolen in the Coincheck hack.[114] Authorities in Japan	Hackers stole 523 million NEM coins from an address stored in a "Hot Wallet" accessible on the Internet. (Jan. 29, 2018) [115]

[112] Lord Remorin, Beyond Bad Trades: Cybersecurity Risks to Cryptocurrency Exchange Users, TREND MICRO (Sep. 14, 2018) https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/beyond-bad-trades-cybersecurity-risks-to-cryptocurrency-exchange-users#HackedTradingPlatforms.

[113] Robert McMilan, The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster**:** Tokyo-based bitcoin exchange Mt. Gox filed for bankruptcy last week, saying hackers had stolen the equivalent of $460 million from its online coffers. The news rocked the bitcoin world, and it could even bring down the much-hyped digital currency. WIRED (March 3, 2014), https://www.wired.com/2014/03/bitcoin-exchange/.

[114] Sebastian Sinclair, 30 Charged in Japan With Trading $96M of Crypto Stolen in Coincheck Hack (Updated Dec 10, 2022), https://www.coindesk.com/policy/2021/01/22/30-charged-in-japan-with-trading-96m-of-crypto-stolen-in-coincheck-hack/.

[115] Nikhilesh De, Coincheck Confirms Crypto Hack Loss Larger than Mt Gox: Japanese exchange Coincheck has confirmed that about $533 million-worth of cryptocurrency has been stolen from its digital wallets, Coindesk (Jan.

		alleged the people were found to have been exchanging NEM's XEM cryptocurrency for other cryptocurrencies via an illicit exchange on a darknet marketplace.	260,000 users affected.
Aug. 18, 2021	Liquid Japanese Crypto Exchange	According to researchers, $45 million were in Ethereum tokens, which were converted to ether, to prevent the assets from being frozen.	Loss of $97 million in digital coins
Aug. 30, 2021	Cream Finance Taiwanese decentralized finance platform	The hackers exploited a bug and used a reentrancy attack to steal AMP tokens and ETH coins.	Loss of over $29 million in cryptocurrency
Oct. 27, 2021	Cream Finance, Poland Decentralized finance ("DeFi") platform	In their third attack of 2021, attackers exploited a vulnerability in the platform's lending system (flash loaning) to steal all of their assets and tokens running on the Ethereum blockchain.	$130 million theft
Nov. 6, 2021	bZx Decentralized finance platform that allows users to borrow, loan, and speculate on cryptocurrency price variations.	bZx phishing attack; cryptocurrency theft. A bZx developer was sent a phishing email with a malicious Word document attached. Threat actors compromised the developer's mnemonic wallet phrase and emptied their personal wallet before stealing two private keys for bZx's Polygon and Binance Smart Chain (BSC) blockchains.	Stole an estimated $55 million
Dec. 1, 2021	MonoX Finance Blockchain startup	Monox cryptocurrency theft. A threat actor exploited a vulnerability in the software the company used to draft smart contracts. The threat actor was able to inflate the price of the MONO token and use it to cash out all the other deposited tokens.	Lost $31M
Dec. 2, 2021	BadgerDAO Decentralized finance ("DeFi")	BadgerDAO DeFi protocol cyber attack. The DAO paused all smart contracts in order to prevent further withdrawals. Crypto lender Celsius Network subsequently	Hackers stole $120.3 million in crypto.

26, 2018, updated Dec. 11, 2022), https://www.coindesk.com/markets/2018/01/26/coincheck-confirms-crypto-hack-loss-larger-than-mt-gox/

		confirmed the company had lost money from the hack.	
Dec. 12, 2021	AscendEX Crypto Exchange	AscendEX hot wallet breach. Assets were taken across three blockchains—Ethereum, Binance Smart Chain, and Polygon—with stolen tokens including significant amounts of stablecoins. The firm subsequently froze deposits and withdrawals.	Lost $77.7 million in a breach of its hot wallet.
Aug. 2021	Poly Network	A hacker breached the blockchain-based Poly Network platform, which allows users to swap tokens across blockchains.[116] "the hacker exploited a vulnerability, which is the _executeCrossChainTx function between contract calls. Therefore, the attacker uses this function to pass in carefully constructed data to modify the keeper of the EthCrossChainData contract."	Hackers stole more than $600 million in cryptocurrency.
Jan. 17, 2022	Crypto.com	Crypto.com 2FA bypass hack The exchange has subsequently instituted strict 2FA measures a fund restoration program for qualifying users.	Cyber attack led to unauthorized withdrawals of Bitcoin and Ether worth $35 million and affected at least 483 user accounts.
Jan. 27, 2022	Qubit Finance cryptocurrency theft, U.K. Decentralized finance platform	The attackers exploited a vulnerability in one of its Ethereum blockchain contracts. Qubit has offered to pay the attacker a bounty to return the stolen funds.	Threat actors stole $80 million worth of cryptocurrency.
Feb. 8, 2022	Gemini Trust Co. Cryptocurrency exchange IRA Financial Trust	IRA Financial offers self-directed retirement accounts It allows its customers to purchase cryptocurrency through a partnership with the cryptocurrency exchange Gemini Trust Co.	Lost $36 million in cryptocurrency when unknown threat actors drained $21 million in Bitcoin and $15 million in Ethereum from the accounts of IRA customers.

[116] Dan, Gunderman, Poly Network Says $600 Million in Cryptocurrency Stolen: Platform Communicates With Hacker, Who Begins Returning Funds, BANKINFOSECURITY (Aug. 10, 2021), https://www.bankinfosecurity.com/poly-network-says-600-million-in-cryptocurrency-stolen-a-17255. Interestingly after a plea to the hackers to return the assets, the next day it appeared the hacker had returned some of the stolen assets. Experts suggested that because it is difficult to launder and cash out crypto assets because of the transparency of the blockchain, it was easier to return the stolen assets.

Aug. 9, 2022	Curve Finance Integral part of the DeFi ecosystem due to its CRV token rewards emissions, which serve as a source of income for several other protocols.	Curve Finance Hackers changed the DNS ID	$570,000 stolen
	Coindesk	Hackers appear to have changed the domain name system (DNS) entry for the protocol, forwarding users to a fake clone and approving a malicious contract. The contract remained uncompromised.	
Sep. 2022 and June 2022	Wintermute One of largest liquidity providers across most DeFi and DeFi exchanges. Dedicated to crypto market making for exchanges including Binance and Coinbase.	Sept 2022 – Second security-based incident this year. Platform disrupted for several days. June 2022 – A hacker stole Optimism tokens by exploiting a failed transaction. May have been the result of a "hot wallet" compromise due to the Profanity bug discovered. Wallet addresses generated using the Profanity tool were at risk of compromise.	Suffered a major setback in a second security-based incident this year. – Loss $160 million. June 2022 20 million Optimism tokens stolen
Sep. 20, 2022	Blockworks	Hacker exploited a known vulnerability. Suspected attack vector was a bug in vanity address generator Profanity.	
Cross-Chain Vulnerabilities and Bridge Exploits – allows users to transfer their digital assets from crypto network to another.			
Dec. 4, 2021	BitMart, Cayman Islands Global cryptocurrency exchange platform.	Security breach was caused by a stolen private key that affected two of its hot wallets — one hosted on the Ethereum blockchain and the other on the Binance Smart Chain. [117] A hot wallet is an online-accessible wallet for virtual currency. Compared to cold wallets (also called offline wallets), hot wallets offer increased convenience but carry much greater security risks.	Hackers withdrew $150 million in assets.

[117] Crypto Exchange BitMart Loses $150 Million to Hackers (Dec. 8, 2021), TrendMicro, https://news.trendmicro.com/2021/12/08/crypto-exchange-bitmart-loses-150-million-to-hackers/?_ga=2.189076328.2136864251.1671303228-2061427346.1671303227.

		Bitmart says it will reimburse victims for all losses.	
Jan. 17, 2022	Multichain A platform that allows users to swap tokens between blockchains,	Hackers exploited a vulnerability in the blockchain service. One of the attackers is now negotiating with the victims to return 80% of the stolen funds and keep the remaining 20% as a 'tip.'	Lost approximately $1.4 million
Feb. 2, 2022	Wormhole, Switzerland One of the most popular bridges linking the Solana and Ethereum blockchains.	A threat actor launched multiple attacks aimed to bypass the verification process of the Wormhole bridge on Solana and exploit a vulnerability in the platform's smart contracts, By injecting a malicious "message" the attacker successfully minted 320 wETH. Wormhole offered the hacker $10 million in exchange for return of the stolen funds. To this day, the attacker's funds are still sitting in the attacker's wallets.	Lost an estimated $322 million worth of Ether currency. The attacker carried out the second-largest crypto theft from a DeFi protocol ever as of that date (July 2022)
Mar. 23, 2022	Ronin Network Bridge, Canada Used to power the popular online blockchain game Axie Infinity, an NFT-driven game operated by Vietnam-based Sky Mavis.	Attackers breached Ronin Network security by gaining access to private keys they used to forge fake withdrawals. The US subsequently attributed the incident to North Korean state-backed hacking collective Lazarus Group and announced new sanctions against an Ethereum wallet belonging to the group. [118]	Hijacked 173,600 Ethereum and $25.5 million - totaling nearly $615 million in stolen funds. Lost $615 million in ether and USD Coin tokens in the second largest cryptocurrency heist to date.
June 2022	Harmony Launched in 2019, Harmony offers a two-way Ethereum bridge powered by the Harmony One token (ONE).	Bridge exploit on Harmony's Horizon bridge. 12 attack transactions and three attack addresses. How? The attacker gained control of the owner's authority over the MultiSigWallet to call the confirm Transaction() directly to transfer large amounts of tokens from the bridge to Harmony.	Loss of approximately $97M

[118] Trend Micro, *supra* note 34.
https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/beyond-bad-trades-cybersecurity-risks-to-cryptocurrency-exchange-users#HackedTradingPlatforms

		The assets are still being held in the exploiter's address.	
April 17, 2022	Beanstalk Farms Decentralized finance platform	"Flash loan" exploit. The attackers took out a large loan, to acquire enough voting rights to make the necessary governance changes to move all of Beanstalk's reserves. The price of each Bean has since plummeted to near zero before coming back up to around one dollar.	Lost $180 million in cryptocurrency
	Mango Market Solana-based Aave crypto-lending platform	Hacked by Avi Eisenberg who "took over the platform." He did nothing illegal, "worked within the parameters of the project's code. Exploited the platform by swapping out CRV tokens for loans."	Loss of $100 million
Aug. 2022	Nomad Crypto bridge protocol	Flawed software/code upgrade. "Hackers struck after a routine upgrade allowed verification messages to be bypassed," allowing the attacker "to essentially copy/paste transactions and subsequently drain the bridge of nearly all its funds over a long series of transactions before it could be stopped." Impersonators posed as Nomad and provided fraudulent addresses to collect funds.	Stole $190 million
	Axie Liberty	Breach of foreign crypto wallets. No Korea phishing attack, transferred funds through crypto-mixers, converted into cash.	